

SHOW FILES;DS
File 2:INSPEC 1969-2002/Jan W1
(c) 2002 Institution of Electrical Engineers
File 6:NTIS 1964-2002/Jan W3
(c) 2002 NTIS, Intl Cpyrght All Rights Res
File 8:Ei Compendex(R) 1970-2002/Jan W1
(c) 2002 Engineering Info. Inc.
File 34:SciSearch(R) Cited Ref Sci 1990-2002/Jan W1
(c) 2002 Inst for Sci Info
File 35:Dissertation Abs Online 1861-2002/Jan
(c) 2002 ProQuest Info&Learning
File 65:Inside Conferences 1993-2002/Jan W1
(c) 2002 BLDSC all rts. reserv.
File 77:Conference Papers Index 1973-2002/Jan
(c) 2002 Cambridge Sci Abs
File 92:IHS Intl.Stds.& Specs. 1999/Nov
(c) 1999 Information Handling Services
File 94:JICST-EPlus 1985-2002/Nov W4
(c)2002 Japan Science and Tech Corp(JST)
File 95:TEME-Technology & Management 1989-2002/JAN W1
(c) 2002 FIZ TECHNIK
File 99:Wilson Appl. Sci & Tech Abs 1983-2001/Nov
(c) 2001 The HW Wilson Co.
File 103:Energy SciTec 1974-2001/Sep B2
(c) 2001 Contains copyrighted material
File 108:AEROSPACE DATABASE 1962-2001/DEC
(c) 2001 AIAA
File 144:Pascal 1973-2002/Dec W5
(c) 2002 INIST/CNRS
File 202:Information Science Abs. 1966-2001/ISSUE 09
(c) Information Today, Inc
File 233:Internet & Personal Comp. Abs. 1981-2002/Jan
(c) 2002 Info. Today Inc.
File 238:Abs. in New Tech & Eng. 1981-2001/Dec
(c) 2001 Reed-Elsevier (UK) Ltd.
File 239:Mathsci 1940-2001/Feb
(c) 2001 American Mathematical Society
File 275:Gale Group Computer DB(TM) 1983-2002/Jan 09
(c) 2002 The Gale Group
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 647:CMP Computer Fulltext 1988-2002/Dec W4
(c) 2002 CMP Media, LLC
File 674:Computer News Fulltext 1989-2001/Dec W2
(c) 2001 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2002/Jan 08
(c) 2002 The Dialog Corp.
File 9:Business & Industry(R) Jul/1994-2002/Jan 08
(c) 2002 Resp. DB Svcs.
File 15:ABI/Inform(R) 1971-2002/Jan 07
(c) 2002 ProQuest Info&Learning
File 16:Gale Group PROMT(R) 1990-2002/Jan 08
(c) 2002 The Gale Group
File 18:Gale Group F&S Index(R) 1988-2002/Jan 08
(c) 2002 The Gale Group
File 20:Dialog Global Reporter 1997-2002/Jan 09
(c) 2002 The Dialog Corp.
File 80:TGG Aerospace/Def.Mkts(R) 1986-2002/Jan 08
(c) 2002 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2002/Jan 08
(c)2002 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 256:SoftBase:Reviews,Companies&Prods. 85-2002/Dec
(c)2002 Info.Sources Inc

File 481:DELPHEES Eur Bus 95-2002/Dec W3
(c) 2002 ACFCI & Chambre CommInd Paris
File 583:Gale Group Globalbase(TM) 1986-2002/Jan 08
(c) 2002 The Gale Group
File 621:Gale Group New Prod. Annou.(R) 1985-2002/Jan 08
(c) 2002 The Gale Group
File 624:McGraw-Hill Publications 1985-2002/Jan 09
(c) 2002 McGraw-Hill Co. Inc
File 635:Business Dateline(R) 1985-2002/Jan 08
(c) 2002 ProQuest Info&Learning

Set	Items	Description
S1	33	AU=((KOCHER P) OR (KOCHER P C) OR (KOCHER, PAUL) OR (KOCHER P. C.))
S2	33	AU=((KOCHER P) OR (KOCHER P C) OR (KOCHER, PAUL) OR (KOCHER P.C.))
S3	33	AU=((KOCHER P) OR (KOCHER P C) OR (KOCHER, PAUL) OR (KOCHER P.C.))
S4	36	AU=((KOCHER P) OR (KOCHER P C) OR (KOCHER, PAUL) OR (KOCHE- R, P.C.))
S5	29	RD S4 (unique items)
?		

T S5/3/1-29

5/3/1 (Item 1 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6047572 INSPEC Abstract Number: B9811-6120B-102, C9811-6130S-098

Title: On certificate revocation and validation

Author(s): Kocher, P.C.

Author Affiliation: ValiCert, Palo Alto, CA, USA

Conference Title: Financial Cryptography. Second International
Conference, FC'98 Proceedings p.172-7

Editor(s): Hirschfeld, R.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1998 Country of Publication: Germany viii+310 pp.

ISBN: 3 540 64951 4 Material Identity Number: XX98-02399

Conference Title: Financial Cryptography. Second International
Conference, FC'98. Proceedings

Conference Date: 23-25 Feb. 1998 Conference Location: Anguilla

Language: English

Subfile: B C

Copyright 1998, IEE

5/3/2 (Item 2 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

5363336 INSPEC Abstract Number: B9610-6120B-066, C9610-6130S-033

Title: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems

Author(s): Kocher, P.C.

Conference Title: Advances in Cryptology - CRYPTO'96. 16th Annual
International Cryptology Conference. Proceedings p.104-13

Editor(s): Koblitz, N.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1996 Country of Publication: West Germany xii+415
pp.

ISBN: 3 540 61512 1 Material Identity Number: XX96-02286

Conference Title: Advances in Cryptology - CRYPTO '96

Conference Sponsor: Int. Assoc. Cryptologic Res.; IEEE; Univ. California

Conference Date: 18-22 Aug. 1996 Conference Location: Santa Barbara,
CA, USA

Language: English

Subfile: B C

Copyright 1996, IEE

5/3/3 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

5120099 INSPEC Abstract Number: B9601-6120B-032, C9601-6130S-025

Title: A known plaintext attack on the PKZIP

Author(s): Biham, E.; Kocher, P.C.

Author Affiliation: Dept. of Comput. Sci., Technion-Israel Inst. of
Technol., Haifa, Israel

Conference Title: Fast Software Encryption. Second International
Workshop. Proceedings p.144-53

Editor(s): Preneel, B.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1995 Country of Publication: West Germany vii+366
pp.

ISBN: 3 540 60590 8

Conference Title: Fast Software Encryption. Second International Workshop. Proceedings
Conference Sponsor: Europay Int.; Microsoft; Uti-maco Belgium
Conference Date: 14-16 Dec. 1994 Conference Location: Leuven, Belgium
Language: English
Subfile: B C
Copyright 1995, IEE

5/3/4 (Item 1 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

10185611 Genuine Article#: 493RK No. References: 9
Title: Zn-K EXAFS investigations on ZnS/ZnO containing vitrified ashes from municipal incinerator facilities
Author(s): Mosel G (REPRINT) ; Hubert T; Nofz M; Brenneis R; Kocher P; Kley G
Corporate Source: Fed Inst Mat Res & Testing BAM, Unter Eichen 44-46/D-12203 Berlin//Germany/ (REPRINT); Fed Inst Mat Res & Testing BAM, D-12203 Berlin//Germany/
Journal: JOURNAL OF MATERIALS SCIENCE, 2001, V36, N20 (OCT), P5017-5025
ISSN: 0022-2461 Publication date: 20011000
Publisher: KLUWER ACADEMIC PUBL, SPUIBOULEVARD 50, PO BOX 17, 3300 AA DORDRECHT, NETHERLANDS
Language: English Document Type: ARTICLE (ABSTRACT AVAILABLE)

5/3/5 (Item 2 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

09229793 Genuine Article#: 382AF No. References: 4
Title: Fabrication of a surface pattern in zirconia
Author(s): Schonholzer UP (REPRINT) ; Filser F; Kocher P; Gauckler LJ
Corporate Source: SWISS FED INST TECHNOL, DEPT MAT SCI/ZURICH//SWITZERLAND/ (REPRINT)
Journal: AMERICAN CERAMIC SOCIETY BULLETIN, 2000, V79, N12 (DEC), P45-47
ISSN: 0002-7812 Publication date: 20001200
Publisher: AMER CERAMIC SOC, 735 CERAMIC PLACE, PO BOX 6136, WESTERVILLE, OH 43081-6136
Language: English Document Type: ARTICLE

5/3/6 (Item 3 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

08170838 Genuine Article#: 253TD No. References: 0
Title: Software
Author(s): Beberg AL; Berger B; Blundin D; Brand M; Brewer E; Chessell M; Freeman E; DeIcaza M; Gee D; Hellerstein J; Isard MA; Jones C; Jurvetson S; Klaus C; Kocher P; Mccue M; Pinckney T; Saul L; Savoie CJ; Saylor MJ; Sweldens W; Torvalds L
Journal: TECHNOLOGY REVIEW, 1999, V102, N6 (NOV-DEC), P74-&
ISSN: 0040-1692 Publication date: 19991100
Publisher: MASS INST TECHNOL, BUILDING W59, CAMBRIDGE, MA 02139
Language: English Document Type: ARTICLE

5/3/7 (Item 4 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

07931719 Genuine Article#: 225LW No. References: 8
**Title: A high-temperature furnace for X-ray diffraction with directly
machined alpha-Al₂O₃ ceramic parts**
Author(s): Estermann M (REPRINT) ; Reifler H; Steurer W; Filser F; Kocher P
; Gauckler LJ
Corporate Source: ETH ZURICH, LAB KRISTALLOG/CH-8092 ZURICH//SWITZERLAND/
(REPRINT)
Journal: JOURNAL OF APPLIED CRYSTALLOGRAPHY, 1999, V32, 4 (AUG 1), P833-836
ISSN: 0021-8898 Publication date: 19990801
Publisher: MUNKSGAARD INT PUBL LTD, 35 NORRE SOGADE, PO BOX 2148, DK-1016
COPENHAGEN, DENMARK
Language: English Document Type: ARTICLE (ABSTRACT AVAILABLE)

5/3/8 (Item 5 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

04862833 Genuine Article#: UN010 No. References: 1
**Title: DESIGN OF A LINEAR ROBUST PSS FOR OPTIMAL DAMPING OF
MULTIMODE-OSCILLATIONS (VOL 6, PG 67, 1996)**
Author(s): HUWER R; KOCHER P; NELLES D; WACHE M
Journal: EUROPEAN TRANSACTIONS ON ELECTRICAL POWER, 1996, V6, N2 (MAR-APR)
, P138
ISSN: 1430-144X
Language: ENGLISH Document Type: CORRECTION, ADDITION

5/3/9 (Item 6 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

04401215 Genuine Article#: TA363 No. References: 19
**Title: PERCUTANEOUS RENAL BIOPSY - A SINGLE-CENTER EXPERIENCE WITH
AUTOMATED SPRING-LOADED GUN TYPE DEVICE**
Author(s): BALLAL SH; NAYAK R; DHANRAJ P; KOCHER P; BASTANI B
Corporate Source: ST LOUIS UNIV, HLTH SCI CTR, DIV NEPHROL, 3635 VISTA
AVE, 9N-FDT/ST LOUIS//MO/63110; ST LOUIS UNIV, HLTH SCI CTR, DIV
NEPHROL/ST LOUIS//MO/63110; MANIPAL HOSP/BANGALORE/KARNATAKA/INDIA/
Journal: CLINICAL NEPHROLOGY, 1995, V44, N4 (OCT), P274-275
ISSN: 0301-0430
Language: ENGLISH Document Type: NOTE

5/3/10 (Item 1 from file: 103)

DIALOG(R)File 103:Energy SciTec
(c) 2001 Contains copyrighted material. All rts. reserv.

03672525 DE-94-0G7885; EDB-94-088491
**Title: Method for the load-dependent control of flow temperature of a
heating system**
Original Title: Ein Verfahren zur lastgefuehrten Regelung der
Heizungs-Vorlauftemperatur
Author(s): Kocher, P.
Source: HLH, Heizung, Lueftung, Klimatechnik, Haustechnik (Germany) v
45:1. Coden: HLHZAS ISSN: 0017-9906
Publication Date: Jan 1994 p 7-9
Language: German

5/3/11 (Item 2 from file: 103)

DIALOG(R)File 103:Energy SciTec
(c) 2001 Contains copyrighted material. All rts. reserv.

03619502 AIX-25-010778; EDB-94-035468

Title: Real-time modelling of a ventilation system for a power plant simulator

Author(s): Kocher, P.; Welfonder, E. (Stuttgart Univ. (Germany). Dept. of Power Generation and Automatic Control)

Title: Control of power plants and power systems

Author(s)/Editor(s): Welfonder, E. (Stuttgart Univ. (Germany). Dept. of Power Generation and Automatic Control); Lausterer, G.K. (Siemens AG, Karlsruhe (Germany)); Weber, H. (eds.) (Elektrizitaetswerk Laufenburg AG (Switzerland))

Original Series Title: IFAC Symposia Series, no. 9

Corporate Source: International Federation of Automatic Control (IFAC), Duesseldorf (Germany)

Conference Title: International IFAC symposium on control of power plants and power systems

Conference Location: Munich (Germany) Conference Date: 9-11 Mar 1992

Publisher: Oxford (United Kingdom) Pergamon Press

Publication Date: 1992 p 55-62 (499 p)

Report Number(s): CONF-920312--

ISBN: 0-08-041709-4

Language: English

5/3/12 (Item 3 from file: 103)

DIALOG(R)File 103:Energy SciTec

(c) 2001 Contains copyrighted material. All rts. reserv.

03211755 DEN-91-008972; EDB-91-139191

Title: Article on realtime simulation of energy-specific processes using a ventilation system of a nuclear power station

Original Title: Beitrag zur Echtzeitsimulation energietechnischer Prozesse am Beispiel des Lueftungssystems eines Kernkraftwerks

Author(s)/Editor(s): Kocher, P.

Corporate Source: Stuttgart Univ. (Germany). Fakultae 5 - Energietechnik

Publication Date: 25 Jun 1990 (195 p)

Language: In German

5/3/13 (Item 4 from file: 103)

DIALOG(R)File 103:Energy SciTec

(c) 2001 Contains copyrighted material. All rts. reserv.

01202886 EDB-83-102923

Author(s): Kocher, P.

Title: Energy information guidance manual

Corporate Source: New York Inst. of Tech., Old Westbury (USA). Center for Energy Policy and Research

Publication Date: 1982 p 310

Report Number(s): DOE/CS/69160-T5

Order Number: DE83012830

Contract Number (DOE): FG03-81CS69160

Language: English

5/3/14 (Item 1 from file: 144)

DIALOG(R)File 144:Pascal

(c) 2002 INIST/CNRS. All rts. reserv.

14245305 PASCAL No.: 99-0448035

A high-temperature furnace for X-ray diffraction with directly machined alpha -Al SUB 2 O SUB 3 ceramic parts

ESTERMANN M; REIFLER H; STEURER W; FILSER F; KOCHER P; GAUCKLER L J

Laboratorium fuer Kristallographie, Eidgenoessische Technische Hochschule ETH, 8092 Zuerich, Switzerland; Nichtmetallische Werkstoffe,

Eidgenoessische Technische Hochschule ETH, 8092 Zuerich, Switzerland
Journal: Journal of applied crystallography, 1999, 32 (p.4) 833-836
Language: English

Copyright (c) 1999 INIST-CNRS. All rights reserved.

5/3/15 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

14245243 PASCAL No.: 99-0447972
Differential power analysis
CRYPTO '99 : advances in cryptology : Santa Barbara CA, 15-19 August 1999
KOCHER P; JAFFE J; JUN B
WIENER Michael, ed
Cryptography Research, Inc., 870 Market Street, Suite 1088, San
Francisco, CA 94102, United States
Annual international cryptology conference, 19 (Santa Barbara CA USA)
1999-08-15
Journal: Lecture notes in computer science, 1999, 1666 388-397
Language: English

Copyright (c) 1999 INIST-CNRS. All rights reserved.

5/3/16 (Item 3 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

11505112 PASCAL No.: 94-0345714
Recrutement des donneus de sang : nouvelle strategie
(Recruitment of blood donors : new strategies)
KOCHER P
CTS neuchatelois jurassien CRS, 2300 La Chaux-de-Fonds, Switzerland
Journal: Medecine et hygiene, 1994, 52 (2024) 1000-1005 (4 p.)
Language: French Summary Language: English

5/3/17 (Item 4 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

11031768 PASCAL No.: 93-0541275
La psychanalyse en Europe centrale et sa mouvance vers l'Occident pendant les annees vingt et trente
(Central European psychoanalysis and its more westward in the twenties and thirties)
HAYNAL A; KOCHER P trad
Fac. medecine, dep. psychiatrie, Geneve, Switzerland
Journal: Psychotherapies, 1993, 13 (2) 99-106
Language: French Summary Language: English

5/3/18 (Item 5 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

08648138 PASCAL No.: 89-0197358
Vollstaendige Modale Synthese optimaler Zustandsregelungen
(Synthese modale complete des systemes de commande optimaux a boucle de reaction d'etat)
(Complete modal synthesis of optimal state feedback controllers)
ROPPENECKER G; KOCHER P

Univ. Karlsruhe, inst. regelungs steuerungssysteme, Karlsruhe 6750,
Federal Republic of Germany
Journal: Automatisierungstechnik, 1988, 36 (8) 295-300
Language: German Summary Language: English

5/3/19 (Item 6 from file: 144)

DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

08180187 PASCAL No.: 88-0180537

Sero-epidemiological survey for alveolar echinococcosis (by Em2-ELISA) of blood donors in an endemic area of Switzerland

GOTTSTEIN B; LENGELER C; BACHMANN P; HAGEMANN P; KOCHER P; BROSSARD M;
WITASSEK F; ECKERT J

Univ. Zuerich, inst. parasitology, Zuerich 8057, Switzerland

Journal: Transactions of the Royal Society of tropical Medicine and Hygiene, 1987, 81 (6) 960-964

Language: ENGLISH

5/3/20 (Item 7 from file: 144)

DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

05177309 PASCAL No.: 83-0441173

Le nouvel emetteur a ondes courtes de 500 kW

KOCHER P; TOMLJENOVIC J

Journal: Revue Brown Boveri, 1983, 70 (5-6) 235-240

Language: French

5/3/21 (Item 8 from file: 144)

DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

03726369 PASCAL No.: 82-0245563

HOMOSEXUALITE EN 1982. I: REVUE

HAYNAL A; KOCHER P

CENT. PSYCHO-SOCIAL UNIV./GENEVE 1211, SWITZERLAND

Journal: MED. HYG., 1982, 40 (1465) 1274-1285 7 P.

Language: FRENCH

5/3/22 (Item 9 from file: 144)

DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

02881232 PASCAL No.: 80-0155008

DER EINFLUSS DER GLASPHASE AUF DIE EIGENSCHAFTEN SCHMELZGEGOSSENER ZIRKON-KORUND-STEINE

(L'INFLUENCE DE LA PHASE VITREUSE SUR LES PROPRIETES DE BRIQUES REFRACTAIRES CORINDON-ZIRCONE)

MIELDS R; SCHRODER W; KOCHER P; FRISCHBUTTER E

AKAD. WISS. DDR, ZENTRALINST. ANORGAN. CHEM., GERMAN DEMOCRATIC REPUBLIC

Journal: SILIKATTECHNIK, 1979, 30 (9) 273-276

Language: GERMAN Summary Language: RUSSIAN; ENGLISH; FRENCH

5/3/23 (Item 10 from file: 144)

DIALOG(R)File 144:Pascal
(c) 2002 INIST/CNRS. All rts. reserv.

02265990 PASCAL No.: 79-0212378

TRAITEMENT D'URGENCE DES DIATHESES HEMORRAGIQUES

KOCHER P

SERVICE NEUCHATELOIS JURASSIEN TRANSFUSION SANGUINE, LA CHAUX-DE-FONDS
2300, SWITZERLAND

Journal: REV. MED. SUISSE ROMANDE, 1978, 98 (12) 659-663

Language: FRENCH

5/3/24 (Item 11 from file: 144)

DIALOG(R)File 144:Pascal

(c) 2002 INIST/CNRS. All rts. reserv.

00365944 PASCAL No.: 73-0001971

L'EXPLORATION DES ANEMIES

KOCHER P

HOP. LA CHAUX-DE-FONDS, 2300 LA CHAUX-DE-FONDS

Journal: REV. MED. SUISSE ROMANDE, 1973, 93 (3) 163-173

Language: FRENCH

5/3/25 (Item 1 from file: 434)

DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

(c) 1998 Inst for Sci Info. All rts. reserv.

05997969 Genuine Article#: TH697 No. References: 6

Title: SEROLOGY OF BLOOD-GROUPS FOR PRACTICAL BLOOD-TRANSFUSION

Author(s): KOCHER P

Corporate Source: CRS, CTR TRANSFUS, SOPHIE MAIRET 28/CH-2300 LA CHAUX DE
FONDS//SWITZERLAND/Journal: THERAPEUTISCHE UMSCHAU REVUE THERAPEUTIQUE, 1984, V41, N8, P
576-581

Language: FRENCH Document Type: ARTICLE

5/3/26 (Item 2 from file: 434)

DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

(c) 1998 Inst for Sci Info. All rts. reserv.

05997964 Genuine Article#: TH697 No. References: 9

Title: RED BLOOD-CELLS - INDICATIONS AND APPLICATIONS

Author(s): KOCHER P

Corporate Source: CTR NEUCHATELOIS & JURASSIEN TRANSFUS SANGUINE, SOPHIE
MAIRET 28/CH-2300 LA CHAUX DE FONDS//SWITZERLAND/Journal: THERAPEUTISCHE UMSCHAU REVUE THERAPEUTIQUE, 1984, V41, N8, P
549-553

Language: FRENCH Document Type: ARTICLE

5/3/27 (Item 3 from file: 434)

DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

(c) 1998 Inst for Sci Info. All rts. reserv.

05279061 Genuine Article#: RC385 No. References: 9

Title: A NEW 500 KW SHORT-WAVE TRANSMITTER

Author(s): KOCHER P; TOMLJENOVIC J

Corporate Source: BROWN BOVERI & CO LTD/CH-5401 BADEN//SWITZERLAND/

Journal: BROWN BOVERI REVIEW, 1983, V70, N5-6, P235-240

Language: ENGLISH Document Type: ARTICLE

5/3/28 (Item 4 from file: 434)

DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

(c) 1998 Inst for Sci Info. All rts. reserv.

02557011 Genuine Article#: GT930 No. References: 23

**Title: PROGNOSTIC FACTORS FOR SURVIVAL AND TUMOR RECURRENCE FOLLOWING
SURGERY AND RADIOTHERAPY OF BREAST-CANCER WITH POSITIVE AXILLARY NODES,
LA CHAUX-DE-FONDS, 1968-1975**

Author(s): BAUMGARTNER JD; ALBERTO P; KOCHER P

Corporate Source: UNIV GENEVA, DIV ONCO HEMATOL/CH-1211 GENEVA
4//SWITZERLAND/; HOP CHAUX DE FONDS, SERV MED/CHAUX DE
FONDS//SWITZERLAND/

Journal: SCHWEIZERISCHE MEDIZINISCHE WOCHENSCHRIFT, 1979, V109, N18, P
681-688

Language: FRENCH Document Type: ARTICLE

5/3/29 (Item 5 from file: 434)

DIALOG(R)File 434:SciSearch(R) Cited Ref Sci

(c) 1998 Inst for Sci Info. All rts. reserv.

00634226 Genuine Article#: AE489 No. References: 0

Title: INTEGRATING BLOOD-TRANSFUSION SERVICE INTO HOSPITAL STRUCTURE

Author(s): SIEGENTHALER P; KOCHER P

Corporate Source: CTR TRANSF SANGUINE, 42 CLOS BROCHET/CH-2000
NEHATEL//SWITZERLAND/

Journal: SCHWEIZERISCHE MEDIZINISCHE WOCHENSCHRIFT, 1975, V105, N24, P
788-790

Language: FRENCH Document Type: ARTICLE

?

Set	Items	Description
S1	95	(HASH OR AUTHENTIC? OR MERKLE) (W) TREE?
S2	6725	(REVOCATION OR REVOK? OR EXPIR?) (5N) CERTIFICAT?
S3	15	S2 AND S1
S4	9	RD S3 (unique items)
S5	82633	CRT
S6	172	S2 (3N) TREE?
S7	76	RD S6 (unique items)

7/9/1 (Item 1 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

7112544 INSPEC Abstract Number: B2002-01-6120D-087, C2002-01-1260C-069

Title: Certificate revocation protocol using k-ary hash tree

Author(s): Kikuchi, H.; Abe, K.; Nakanishi, S.

Author Affiliation: Dept. of Electr. Eng., Tokai Univ., Hiratsuka, Japan

Journal: IEICE Transactions on Communications vol.E84-B, no.8 p.

2026-32

Publisher: Inst. Electron. Inf. & Commun. Eng,

Publication Date: Aug. 2001 Country of Publication: Japan

CODEN: ITCMEZ ISSN: 0916-8516

SICI: 0916-8516(200108)E84B:8L.2026:CRPU;1-2

Material Identity Number: P711-2001-011

Language: English Document Type: Journal Paper (JP)

Treatment: Theoretical (T)

Abstract: Certificate revocation is a critical issue for a practical, public-key infrastructure. A new efficient revocation protocol using a one-way hash tree structure (instead of the classical list structure, which is known as a standard for revocation), was proposed and examined to reduce communication and computation costs. We analysis a k-ary hash tree for certificate revocation and prove that k=2 minimizes communication cost. (22 Refs)

Subfile: B C

Descriptors: certification; message authentication; protocols; public key cryptography; tree data structures

Identifiers: certificate revocation protocol; k-ary hash tree; public-key infrastructure; communication cost minimization

Class Codes: B6120D (Cryptography); B6150M (Protocols); C1260C (Cryptography theory); C6130S (Data security); C6120 (File organisation); C5640 (Protocols)

Copyright 2001, IEE

7/9/2 (Item 2 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

7094869 INSPEC Abstract Number: B2002-01-6120D-004, C2002-01-6130S-008

Title: Threaded binary sorted hash trees solution scheme for certificate revocation problem

Author(s): Wang Shang-ping; Mang Ya-ling; Wang Yu-min

Author Affiliation: Nat. Key Lab. on ISN, Xidian Univ., Xi'an, China

Journal: Journal of Software vol.12, no.9 p.1341-50

Publisher: Science Press,

Publication Date: Sept. 2001 Country of Publication: China

CODEN: RUXUEW ISSN: 1000-9825

SICI: 1000-9825(200109)12:9L.1341:TBSH;1-A

Material Identity Number: G255-2001-010

Language: Chinese Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: A new solution scheme called certificate revocation threaded binary sorted hash trees (CRTBSHT) for the certificate revocation problem

in public key infrastructure (PKI) is proposed. Previous solution schemes include: traditional X.509 certificate system's certificate revocation lists (CRL), S. Micali's (1996) Certificate Revocation System (CRS), P. Kocher's (1998) Certificate Revocation Trees (CRT). and Naor-Nissim's 2-3 certificate revocation trees (2-3 CRT) (M. Naor and K. Nissim, 2000) but none is perfect. The new scheme keeps the best properties of CRT, i.e., it is easy to check or prove whether a certificate is revoked which only needs related path values but does not need the whole CRT values and overcomes the disadvantage of CRT that any update will cause the whole CRT to be computed completely. The new scheme has referential value to PKI engineering practice. (7 Refs)

Subfile: B C

Descriptors: certification; message authentication; public key cryptography; sorting; trees (mathematics)

Identifiers: threaded binary sorted hash tree solution scheme; certificate revocation problem; CRTBSHT; public key infrastructure; PKI; Certificate Revocation System; Certificate Revocation Trees; 2-3 certificate revocation tree; related path values; referential value; PKI engineering practice; certification authority; digital signature

Class Codes: B6120D (Cryptography); B0250 (Combinatorial mathematics); C6130S (Data security); C0310D (Computer installation management); C1160 (Combinatorial mathematics)

Copyright 2001, IEE

7/9/3 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

7062769 INSPEC Abstract Number: C2001-11-6130S-050

Title: Asynchronous large-scale certification based on certificate verification trees

Author(s): Domingo-Ferrer, J.; Alba, M.; Sebe, F.

Author Affiliation: Dept. of Comput. Eng. & Math., Univ. Rovira i Virgili, Tarragona, Spain

Conference Title: Communications and Multimedia Security Issues of the New Century. IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CSM'01) p.185-96

Editor(s): Steinmetz, R.; Dittmann, J.; Steinebach, M.

Publisher: Kluwer Academic Publishers, Norwell, MA, USA

Publication Date: 2001 Country of Publication: USA x+393+34 pp.

ISBN: 0 7923 7365 0 Material Identity Number: XX-2001-01927

Conference Title: Communications and Multimedia Security Issues of the New Century. IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01)

Conference Date: 21-22 May 2001 Conference Location: Darmstadt, Germany

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: Good public-key infrastructures (PKI) are essential to make electronic commerce secure. Quite recently, certificate verification trees (CVT) have been introduced as a tool for implementation of large-scale certification authorities (CA). In most aspects, the CVT approach outperforms previous approaches like X.509 and certificate revocation lists, SDSI/SPKI, certificate revocation trees, etc. However, there is a trade-off between manageability for the CA and response time for the user: CVT-based certification as initially proposed is synchronous, ie, certificates are only issued and revoked at the end of a CVT update period (typically once a day). Assuming that the user is represented by a smart card, we present solutions that preserve all advantages of CVT while relaxing the aforementioned synchronization requirement. If short-validity certificates are used, implicit revocation provided by the proposed solutions completely eliminates the need for the signature verifier to check any revocation information (CRL, CRT, etc.). (10 Refs)

Subfile: C

Descriptors: authorisation; certification; electronic commerce; public key cryptography; smart cards; tree searching

Identifiers: asynchronous large-scale certification; certificate verification trees; public-key infrastructures; PKI; secure electronic commerce; large-scale certification authorities; smart card; short-validity certificates; implicit revocation

Class Codes: C6130S (Data security); C7120 (Financial computing); C6120 (File organisation)

Copyright 2001, IEE

7/9/4 (Item 4 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6635492 INSPEC Abstract Number: B2000-08-6120D-015, C2000-08-6130S-021
Title: Performance evaluation of certificate revocation using k-valued

hash tree

Author(s): Kikuchi, H.; Abe, K.; Nakanishi, S.

Author Affiliation: Dept. of Electr. Eng., Tokai Univ., Kanagawa, Japan

Conference Title: Information Security. Second International Workshop, ISW'99. Proceedings (Lecture Notes in Computer Science Vol.1729) p. 103-17

Editor(s): Mambo, M.; Zheng, Y.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1999 Country of Publication: Germany ix+275 pp.

ISBN: 3 540 66695 8 Material Identity Number: XX-1999-03277

Conference Title: Information Security. Second International Workshop, ISW'99. Proceedings

Conference Date: 6-7 Nov. 1999 Conference Location: Kuala Lumpur, Malaysia

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: A CRL (certificate revocation list) defined in X.509 is currently used for certificate revocation. There are some issues of CRL including high communication cost and low latency for update. To solve the issues, there are many proposals including CRT (certificate revocation tree), authenticated dictionary, and delta list. In this paper, we study CRT using k-valued hash tree. To estimate the optimal value of k, we examine the overhead of computation and the communication cost. We also discuss when a CRT should be reduced by eliminating unnecessary entries that have already expired. (19 Refs)

Subfile: B C

Descriptors: certification; public key cryptography

Identifiers: performance evaluation; certificate revocation list; k-valued hash tree; X.509; update latency; communication cost; certificate revocation tree; authenticated dictionary; delta list; computation cost

Class Codes: B6120D (Cryptography); C6130S (Data security)

Copyright 2000, IEE

7/9/5 (Item 5 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6592063 INSPEC Abstract Number: B2000-06-6120D-041, C2000-06-1260C-038

Title: Certificate revocation and certificate update

Author(s): Naor, M.; Nissim, K.

Author Affiliation: Dept. of Comput. Sci. & Appl. Math., Weizmann Inst. of Sci., Rehovot, Israel

Journal: IEEE Journal on Selected Areas in Communications vol.18, no.4 p.561-70

Publisher: IEEE,

Publication Date: April 2000 Country of Publication: USA

CODEN: ISACEM ISSN: 0733-8716

SICI: 0733-8716(200004)18:4L:561:CRU;1-U

Material Identity Number: D958-2000-005

U.S. Copyright Clearance Center Code: 0733-8716/2000/\$10.00

Document Number: S0733-8716(00)01522-5

Language: English Document Type: Journal Paper (JP)

Treatment: Theoretical (T)

Abstract: We present a solution for the problem of certificate revocation. This solution represents certificate revocation lists by authenticated dictionaries that support: (1) efficient verification whether a certificate is in the list or not and (2) efficient updates (adding/removing certificates from the list). The suggested solution gains in scalability, communication costs, robustness to parameter changes, and update rate. Comparisons to the following solutions (and variants) are included: "traditional" certificate revocation lists (CRLs), Micali's (see Tech. Memo MIT/LCS/TM-542b, 1996) certificate revocation system (CRS), and Kocher's (see Financial Cryptography-FC'98 Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1998, vol.1465, p.172-7) certificate revocation trees (CRT). We also consider a scenario in which certificates are not revoked, but frequently issued for short-term periods. Based on the authenticated dictionary scheme, a certificate update scheme is presented in which all certificates are updated by a common message. The suggested solutions for certificate revocation and certificate update problems are better than current solutions with respect to communication costs, update rate, and robustness to changes in parameters, and are compatible, e.g., with X.500 certificates. (25 Refs)

Subfile: B C

Descriptors: message authentication; public key cryptography

Identifiers: certificate update; efficient updates; authenticated dictionaries; efficient verification; certificate revocation lists; communication costs; update rate; traditional certificate revocation lists; certificate revocation system; certificate revocation trees; short-term periods; frequently issued certificates; authenticated dictionary; X.500 certificates; parameter changes robustness; public key cryptography; incremental cryptographic schemes; memory checkers

Class Codes: B6120D (Cryptography); C1260C (Cryptography theory); C6130S (Data security)

Copyright 2000, IEE

7/9/6 (Item 6 from file: 2)

DIALOG(R) File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6396786 INSPEC Abstract Number: B1999-12-6120D-068, C1999-12-6130S-032

Title: Performance evaluation of public-key certificate revocation system with balanced hash tree

Author(s): Kikuchi, H.; Abe, K.; Nakanishi, S.

Author Affiliation: Tokai Univ., Kanagawa, Japan

Conference Title: Proceedings of the 1999 ICPP Workshops on Collaboration and Mobile Computing (CMC'99). Group Communications (IWGC). Internet '99 (IWI'99). Industrial Applications on Network Computing (INDAP). Multimedia Network Systems (MMNS). Security (IWSEC). Parallel Computing '99 (IWPC'99). Parallel Execution on Reconfigurable Hardware (PERH) p.204-9

Editor(s): Panda, D.; Takizawa, M.

Publisher: IEEE, Los Alamitos, CA, USA

Publication Date: 1999 Country of Publication: USA xxi+622 pp.

ISBN: 0 7695 0353 5 Material Identity Number: XX-1999-01656

U.S. Copyright Clearance Center Code: 0 7695 0353 5/99/\$10.00

Conference Title: Proceedings of the 1999 ICPP Workshops

Conference Sponsor: Inf. Process. Soc. Japan (IPSJ); Int. Assoc. Comput. & Commun. (IACC); Univ. Aizu, Japan; Ohio State Univ., USA

Conference Date: 21-24 Sept. 1999 Conference Location: Aizu-Wakamatsu, Japan

Language: English Document Type: Conference Paper (PA)

Treatment: Applications (A); Practical (P)

Abstract: A new method for updating certificate revocation trees (CRT) is proposed. Efficient revocation of public-key certificates is a current issue in public-key infrastructure because a traditional certificate revocation list uses a large amount of bandwidth. A certificate revocation tree is a hash tree of revoked certificates and reduces a bandwidth consumption up to $O(\log(n))$. In this paper, an implementation of certificate revocation tree with S-expression is presented and the performance of the system is evaluated in terms of communication and computational costs. To update a CRT, we have two algorithms; (1) random insertion-a new certificate to be revoked is just inserted into the existing tree and (2) balancing updating-balances CRT every time a new certificate is added. (7 Refs)

Subfile: B C

Descriptors: file organisation; performance evaluation; public key cryptography; tree data structures

Identifiers: performance evaluation; public-key certificate revocation system; balanced hash tree; public-key certificates; public-key infrastructure; certificate revocation tree; revoked certificates; S-expression; random insertion

Class Codes: B6120D (Cryptography); C6130S (Data security); C6120 (File organisation); C5470 (Performance evaluation and testing); C5670 (Network performance)

Copyright 1999, IEE

7/9/7 (Item 7 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6047572 INSPEC Abstract Number: B9811-6120B-102, C9811-6130S-098

Title: On certificate revocation and validation

Author(s): Kocher, P.C.

Author Affiliation: ValiCert, Palo Alto, CA, USA

Conference Title: Financial Cryptography. Second International Conference, FC'98 Proceedings p.172-7

Editor(s): Hirschfeld, R.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1998 Country of Publication: Germany viii+310 pp.

ISBN: 3 540 64951 4 Material Identity Number: XX98-02399

Conference Title: Financial Cryptography. Second International Conference, FC'98. Proceedings

Conference Date: 23-25 Feb. 1998 Conference Location: Anguilla

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: Cryptosystems need to check whether the certificates and digital signatures they are given are valid before accepting them. In addition to providing cryptographically secure validity information, certificate revocation systems must satisfy a variety of challenging technical requirements. The traditional revocation techniques of certificate revocation lists (CRLs) and on-line checking are described, as well as a newer technique, certificate revocation trees (CRTs), based on Merkle hash trees. CRTs provide an efficient and highly-scalable way to distribute revocation information. CRT-based systems include tree issuers who compile revocation information. Confirmation issuers who distribute elements from CRTs, and users who accept certificates. CRTs are gaining increased use worldwide for several reasons. They can be used with existing protocols and certificates, and enable the secure, reliable, scalable, and inexpensive validation of certificates (as well as digital signatures and other data). (4 Refs)

Subfile: B C

Descriptors: certification; cryptography; protocols; tree data structures

Identifiers: certificate revocation; certificate validation; cryptosystems; digital signatures; cryptographically secure validity

information; certificate revocation lists; on-line checking; certificate revocation trees; Merkle hash trees; revocation information distribution; tree issuers; revocation information compilation; protocols

Class Codes: B6120B (Codes); C6130S (Data security); C5640 (Protocols); C6120 (File organisation)

Copyright 1998, IEE

7/9/8 (Item 1 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2002 Inst for Sci Info. All rts. reserv.

09130806 Genuine Article#: BQ96E Number of References: 15

Title: Efficient and fresh certification

Author(s): Gassko I (REPRINT) ; Gemnell PS; MacKenzie P

Corporate Source: BELL LABS, LUCENT TECHNOL, 1600 OSGOOD ST/N

ANDOVER//MA/01845 (REPRINT); UNIV NEW MEXICO, DEPT COMP

SCI/ALBUQUERQUE//NM/87131; BELL LABS, INFORMAT SCI RES CTR/MURRAY

HILL//NJ/07974

, 2000, V1751, P342-353

ISSN: 0302-9743 Publication date: 20000000

Publisher: SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, D-14197 BERLIN,
GERMANY LECTURE NOTES IN COMPUTER SCIENCE

Series: LECTURE NOTES IN COMPUTER SCIENCE

Language: English Document Type: ARTICLE

Geographic Location: USA

Journal Subject Category: COMPUTER SCIENCE, THEORY & METHODS

Abstract: Electronic commerce is becoming more and more commonplace, but security is still a major concern. To provide security, a good public-key infrastructure (PKI) is needed. However, PKIs have been slow in developing, with one of the major difficulties being the creation of certification authorities (CAs), and in particular, dealing with the problem of certificate revocation. We propose a new solution to this problem.

Our solution is based on the idea that individually signed certificates provide little information over any significant time period, given that they may be revoked. That is, after a certain amount of time, a certificate is not useful without some more recent knowledge that it has not been revoked. In all previous work, this has either been handled by off-line/on-line schemes, which require costly updates by the CA for every outstanding certificate for every update period, or by certificate revocation lists/trees.

We propose a system called EFFECT (Easy Fast Efficient Certification Technique), which combines the best properties of individual certificates and certificate revocation trees. We show that EFFECT allows CAs to be more secure, even while providing more frequent freshness updates for certificates, and making certification verification extremely lightweight. We compare EFFECT to previously proposed systems, including traditional X.509 certificates and Certificate Revocation Lists (CRLs), SDSI/SPKI, Micali's Certificate Revocation System (CRS), Kocher's Certificate Revocation Trees (CRTs), and Naor and Nissim's 2-3 Certificate Revocation Trees (23CRTs). Finally, we discuss some novel qualities of EFFECT that no previous solution possesses.

Cited References:

P FIN CRYPT, 1998

*PKIX WORK GROUP, INT X 509 PUBL KEY I

ANDERSON R, WHY CRYPTOSYSTEMS FAIL

DIFFIE W, 1976, V22, P644, IEEE T INFORM THEORY

EVEN S, 1996, P35, J CRYPTOL

FRANKEL Y, CRYPTO 97

HERZBERG A, 1997, 4 ACM S COMP COMM SE

JUTLA C, 1996, 2 US WORKSH EL COMM

KELSEY J, ADV CRYPTOLOGY CRYPT
KOCHER P, QUICK INTRO CERTIFIC
KOHNFELDER L, 1978, THESIS MIT
MERKLE R, P218, ADV CRYPTOLOGY CRYPT
MICALI S, 1997, RSA DAT SEC C SAN FR
NAOR M, P US 98
RAGHU N, INTERNET X 509 PUBLI

7/9/9 (Item 1 from file: 94)

DIALOG(R)File 94:JICST-EPlus

(c)2002 Japan Science and Tech Corp(JST). All rts. reserv.

04956300 JICST ACCESSION NUMBER: 01A0757710 FILE SEGMENT: JICST-E
Internet Technology. Certificate Revocation Protocol Using k-Ary Hash Tree.

KIKUCHI H (1); ABE K (1); NAKANISHI S (1)

(1) Tokai Univ., Hitatsuka-shi, Jpn

IEICE Trans Commun(Inst Electron Inf Commun Eng), 2001, VOL.E84-B,NO.8,

PAGE.2026-2032, FIG.8, TBL.2, REF.22

JOURNAL NUMBER: L1369AAW ISSN NO: 0916-8516

UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3

LANGUAGE: English COUNTRY OF PUBLICATION: Japan

DOCUMENT TYPE: Journal

ARTICLE TYPE: Original paper

MEDIA TYPE: Printed Publication

ABSTRACT: Certificate Revocation is a critical issue for a practical, public-key infrastructure. A new efficient revocation protocol using a one-way hash tree structure (instead of the classical list structure, which is known as a standard for revocation), was proposed and examined to reduce communication and computation costs. In this paper, we analysis a k-ary hash tree for certificate revocation and prove that k=2 minimizes communication cost. (author abst.)

DESCRIPTORS: tree search; hash function; cryptography key; authentication; infrastructure; public key cryptography; protocol; computational complexity; cost analysis

BROADER DESCRIPTORS: function(mathematics); mapping(mathematics); cryptogram; rule; business analysis; analysis(separation); analysis

CLASSIFICATION CODE(S): ND02030R

7/9/10 (Item 2 from file: 94)

DIALOG(R)File 94:JICST-EPlus

(c)2002 Japan Science and Tech Corp(JST). All rts. reserv.

04615435 JICST ACCESSION NUMBER: 00A0430671 FILE SEGMENT: JICST-E
Online Certificate Status Verification Server Using Binary Search Hash Tree.

ABE KENSUKE (1); KIKUCHI HIROAKI (1); NAKANISHI SHOHACHIRO (1)

(1) Tokai Univ., Sch. of Eng.

Joho Shori Gakkai Kenkyu Hokoku, 2000, VOL.2000,NO.30(DPS-97 CSEC-8),

PAGE.131-136, FIG.8, TBL.2, REF.17

JOURNAL NUMBER: Z0031BAO ISSN NO: 0919-6072

UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759

LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan

DOCUMENT TYPE: Journal

ARTICLE TYPE: Original paper

MEDIA TYPE: Printed Publication

ABSTRACT: CRT(Certificate Revocation Tree) is a method using hash tree for public-key certificate revocation. In KA98!, we have implemented an experimental CRT system using the S-expression, and shown that its communication cost is smaller than that of CRL. In this paper, we implement an online certificate status verification server using CRT expressed in binary search tree, and examine the system performance in comparison with KA98!. Based on experimental data, we show that the

latency of CRT is smaller than that of CRL. We also estimate the performance of the system to which an actual revocation data derived from a CRL is applied. (author abst.)

DESCRIPTORS: data protection; hashing; authentication; packaging design; tree structure; telecommunication; client server system; speedup; performance evaluation; tree search; binary tree; main memory; cache memory

IDENTIFIERS: Java

BROADER DESCRIPTORS: protection; storage system; method; design; structure; computer system(hardware); system; modification; improvement; evaluation; tree(graph); subgraph; graph; memory(computer); equipment

CLASSIFICATION CODE(S): JD01020V

7/9/11 (Item 3 from file: 94)

DIALOG(R) File 94:JICST-EPlus

(c)2002 Japan Science and Tech Corp(JST). All rts. reserv.

03792520 JICST ACCESSION NUMBER: 98A0986994 FILE SEGMENT: JICST-E

Certificate Revocation and Update Using Binary Hash Tree.

KIKUCHI HIROAKI (1); ABE KENSUKE (1); NAKANISHI SHOHACHIRO (1)

(1) Tokai Univ., Sch. of Eng.

Joho Shori Gakkai Kenkyu Hokoku, 1998, VOL.98,NO.84(DPS-90 CSEC-2),

PAGE.51-56, FIG.9, REF.8

JOURNAL NUMBER: Z0031BAO ISSN NO: 0919-6072

UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759 621.391.037.3

LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan

DOCUMENT TYPE: Journal

ARTICLE TYPE: Original paper

MEDIA TYPE: Printed Publication

ABSTRACT: A CRL(Certificate Revocation List) defined in X.509 is currently used for revocation. To cope with issue of CRL, that includes a high communication cost and low latency for update, OSCP, Delta-CRL, CRT(Certificate Revocation Tree) and Authenticated Directory have been proposed. In this paper, we implement experimental CRT system, and the expected reduction of communication cost in comparison with CRL. We also propose a new update method which is more efficient in communication than Naor's evaluate method. (author abst.)

DESCRIPTORS: computer security; public key cryptography; data update; hashing; binary tree; performance evaluation; data protection

BROADER DESCRIPTORS: security; guarantee; cryptogram; renewal; storage system; method; tree(graph); subgraph; graph; evaluation; protection

CLASSIFICATION CODE(S): JD01020V; ND02030R

7/9/12 (Item 1 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02358252 SUPPLIER NUMBER: 58238832 (THIS IS THE FULL TEXT)

Certifiably safe: ValiCert's Yosi Amram thinks validation services are key to managing digital certificates.(digital certificate validation service provider)(Company Business and Marketing)(Interview)

Nelson, Matthew

InfoWorld, 21, 50, 54

Dec 13, 1999

DOCUMENT TYPE: Interview ISSN: 0199-6649 LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 1505 LINE COUNT: 00121

ABSTRACT: ValiCert Pres and CEO Yosi Amram says there has been an increase in deployment of digital certificate and public-key infrastructure (PKI) systems in the second half of 1999 as businesses and individuals realize the importance of digital certificate validation. Amram points out that

issuing digital certificates is done offline and entails authenticating the entity and binding the person or entity to the certificate, then the certificate is issued to the subscriber and validated by someone the subscriber trusts. A company issuing certificates to its employees uses the certificates to authenticate the employees when they log onto a virtual private network or extranet, for example. When employees leave the company their certificates need to be revoked, so recipients need a way to validate certificates, much like merchants validate credit cards before accepting them as payment. ValiCert provides a scalable, high-performance and automated means of checking the validity of a certificate in real time using client and recipient toolkits along with plug-ins for popular applications.

TEXT:

DIGITAL CERTIFICATES, digital signatures, and public key infrastructure (PKI) systems have become the Holy Grail for identifying users on networks and on the Internet; they present the possibility of verifying a user's identity in transactions and communications. But before digital certificates can see widespread use, some essential problems have to be resolved. Namely, how can it be possible to manage potentially millions of certificates on the Internet and at the same time know which ones are no longer valid. Matthew Nelson, a senior writer at InfoWorld, recently discussed the issue with Yosi Amram, president and chief executive officer of ValiCert, a provider of validation services for digital certificates. Amram discussed scaling issues and the morass of standards that are intended to solve the problem.

InfoWorld: What do you see going on in the marketplace that ValiCert is working with that the IT manager needs to be made aware of?

Amram: We are seeing, over the last six months, an accelerating deployment of pilot phases of digital-certificate and PKI-type infrastructure systems, along with a number of applications, including VPNs (virtual private networks), online banking, secure messaging, and Web-based extranets. And one of the key drivers for the deployment is the use of digital certificates. Along those lines, we're seeing broader recognition and acceptance of the fact that certificates, much like any other credential, can be revoked and need to be validated when being used in order to ensure a more complete and secure PKI infrastructure.

Issuance, mind you, is an offline process that involves authenticating the entity and creating the binding between that person, or entity, and the digital certificate. Those things happen offline. And then, ultimately, a certificate gets issued to a certificate holder, called the subscriber. When that certificate holder, however, now presents that digital certificate to a relying party, then the recipient needs to turn to somebody (they) know that they can trust and validate that certificate.

InfoWorld: What exactly do you mean by validation?

Amram: In particular, we're referring to the fact that the certificate is not revoked. The simplest scenario ... is to imagine a company that's issuing certificates to its employees. Those certificates are being used to authenticate those employees when they're logging into the VPN or some Web extranet application. If employees leave the company, for whatever reason, either they resign or they're fired, their certificates need to be revoked. So, the recipient needs to make sure that the certificate is still valid or active or authorized. In the same way that in the credit card world you have an infrastructure that's been developed where banks issue you a credit card. However, when you go to a merchant and present that credit card at the supermarket or at the restaurant, that merchant needs to know that credit card is good, that you've paid your bills, and that (the) card is not lost or stolen. So they, in an online fashion, swipe your credit card, and through an infrastructure, which involves a point-of-sale device as well as a clearing network, they validate that credit card.

InfoWorld: Is there a problem with validation?

Amram: What ValiCert provides is a scalable, high-performance, and automated way to, in real time during a transaction, check the validity status of a certificate. So we do that through a combination of client- end:

or recipient toolkits and a set of plug-ins for popular applications that we can buy, as well as a validation-authority ... on the service side that provides the response to those queries. And we do that in an open, universal fashion, supporting a number of protocols such as Online Certificate Status Protocol (OCSP), which we helped author in the CRL distribution points. CRLs -- certificate revocation lists -- are basically signed lists by the certificate authority (CA) for all the revoked certificates. As well as our own high-performance technology, called CRTs, which stands for Certificate Revocation Trees. And the result of this is the option that, through the support for ... the client and the server side, as well as the multiprotocol, we can validate any digital certificate from any certificate authority in any application.

InfoWorld: Is it really the case that the certificate authorities and the PKI providers are not providing any means of checking the status of the certificate?

Amram: Many of the certificate authorities are our partners, and they do provide those capabilities through partnerships with ValiCert. What the CAs can do on their own is issue a CRL, ... and they can post that to a directory or to a validation authority that ValiCert hosts. You need that, combined with our toolkit or plug-in or some other client's method, to check the validity of those certificates. And to the extent you need to go beyond the CRL, you need something more robust like OCSP. (Then) you need a validation authority like the ValiCert Enterprise VA that provides support for real-time protocols. CRLs are simply signed lists of all the revoked certificates that the CA gives you. And they do that once every four, eight, or 24 hours.

InfoWorld: That requires large files to be transferred regularly. Are CRLs only temporary?

Amram: That's correct. As you point out, CRLs become very large (when) they include the list of all the revoked certificates. So alternative methods that are more real-time and more network-and bandwidth-efficient, take the CRL and break it down into smaller chunks, as well as OCSP. In the OCSP, which is a protocol that's been adopted now by a consortium of banks rather than downloading the entire list of revoked certificates, you simply ask a yes/no question from a validation authority. That (authority) says if the certificate's ~~valid or not~~ valid in a ~~real-time fashion and~~ signs that response, ~~providing~~ you the assurance that the certificate is valid or not. Now obviously that validation authority needs to work very closely with the certificate authority to get that information in a real-time fashion from the certificate authority who's issuing those certificates and is managing them through their life cycle, including their revocation.

InfoWorld: This updating model sounds similar to the anti-virus updating model. Are validation companies merging technologies ... to provide certificate revocation lists or certificate information on a more updated basis?

Amram: Yes, it's very much a similar issue and problem. Many applications you have now (are) programs that are being downloaded over the network. (They) are signed to identify who the author of that program is. They're signed with a digital certificate that enables you to authenticate the identity of the author of that program before you allow it to go into your network to execute. So you need to check the validity status of those certificates to make sure that the program is a legitimate program and doesn't contain any bad code or malicious code in the form of a virus. So Trend Micro, for example, is incorporating our technology to do the validity checking of that mobile code. We also, earlier this year, announced the partnership with Finjan in a similar type of application and space. So it's very much related to the virus and mobile-code protection.

InfoWorld: Interoperability has become a very hot topic in the technology industry as of late, with the development of LDAP (Lightweight Directory Access Protocol) systems and XML (Extensible Markup Language). What kind of effect is this trend toward interoperability of languages and technology going to have on digital- certificate revocation?

Amram: We think that interoperability is a very important and major theme in deployment of new technology in general in the digital

certificate, and the PKI space in particular. One of the major things that drivers and value-added development provide is addressing the interoperability issue, in particular with regards to validation. So our support for all (of these) various validation protocols -- be they CRLs, which are the legacy model, or some of the more optimized approaches ... as well as our own CRT technology -- ultimately enables enterprises to host in a single validation-authority environment.

InfoWorld: Where do you see certificates, PKI, and validation of those certificates evolving to in the future?

Amram: We see PKI really growing in adoption in the VPN, secure e-mail, Web-based extranet applications, and (in) verification authorities. (They) are becoming the cornerstone of that infrastructure, alongside the certification authorities and the directory, to ensure the validity, status, and interoperability of that infrastructure.

ValiCert, Inc., in Mountain View, Calif., is at www.valicert.com.

COPYRIGHT 1999 InfoWorld Publishing Co.

COMPANY NAMES: Valicert Inc.--Services
GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Company services; Public key encryption; Data security issue
NAMED PERSONS: Amram, Yosi--Interviews
EVENT CODES/NAMES: 360 Services information
PRODUCT/INDUSTRY NAMES: 4811529 (Online Services NEC)
NAICS CODES: 514191 On-Line Information Services
FILE SEGMENT: CD File 275

7/9/13 (Item 2 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02343940 SUPPLIER NUMBER: 56899626 (THIS IS THE FULL TEXT)

ValiCert ups certificate ante.(Enterprise VA Suite 3.0)(Product Announcement)

Kerstetter, Jim

PC Week, 29

Oct 25, 1999

DOCUMENT TYPE: Product Announcement ISSN: 0740-1604 LANGUAGE:

English RECORD TYPE: Fulltext

WORD COUNT: 338 LINE COUNT: 00033

TEXT:

Valicert Inc. is opening its digital certificate validation technology to other applications, such as financials and e-commerce.

Last week, ValiCert released Enterprise VA Suite 3.0. At the center of the upgraded applications suite is Stateful Validation technology, which allows ValiCert customers to add new validation features to their PKIs (public-key infrastructures) through an API.

With Stateful Validation, a company can go beyond the validation of a user's electronic credentials - digital certificates - and do things such as log users for auditing, on-the-fly credit checks for merchants and rules-based authentication for access control.

ValiCert, of Mountain View, Calif., is helping to solve one of the most perplexing parts of PKI: certificate revocation and validation. Each CA (certificate authority), ranging from international CAs such as VeriSign Inc. to CAs managed by companies that do their own PKI distribution, publishes a list of digital certificates that have been revoked, called a CRL (Certificate Revocation List).

About two years ago, ValiCert launched its Certificate Revocation Tree technology that acts as a clearinghouse service for CRL information. At this point, ValiCert has inked deals to handle CRLs from Baltimore Technologies Inc., GTE CyberTrust Solutions Inc., GlobalSign NV, Entegritty Solutions Inc., Entrust Technologies Inc., Microsoft Corp., the Sun/Netscape Alliance, Thawte Certification plc. and Veri Sign.

ValiCert also works with most validation protocols, such as Online

Certificate Status Protocol and CRL Distribution Points.

VA Suite 3.0 comprises four components: Enterprise VA, which allows companies to host certificate revocation data; Validator Suite, a set of plug-ins that allows existing PKI software to check on the revocation status of digital certificates; Validator Tool kit, which allows integration of the revocation-checking technology into other applications; and Publisher, which takes certificate revocation information from outside CAs, publishes them to ValiCert's service center and distributes them to software at corporate sites.

Pricing depends on configuration.

ValiCert can be reached at (650) 567-5400 or www.valicert.com.

COPYRIGHT 1999 Ziff-Davis Publishing Company

COMPANY NAMES: Valicert Inc.--Product introduction
GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Software product introduction; Network security software
EVENT CODES/NAMES: 336 Product introduction
PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software)
NAICS CODES: 51121 Software Publishers
TRADE NAMES: Enterprise Validation Server Suite 3.0 (Network security software)--Product introduction
FILE SEGMENT: CD File 275

7/9/14 (Item 3 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02323680 SUPPLIER NUMBER: 55480853 (THIS IS THE FULL TEXT)

ValiCert simplifies certificate validation. (Validation Authority Service) (Company Business and Marketing)

Kerstetter, Jim

PC Week, 32

August 16, 1999

ISSN: 0740-1604

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 361

LINE COUNT: 00035

TEXT:

Valicert Inc. will expand the reach of its digital certificate revocation technology this week when it unveils the ValiCert Affiliate Program, giving a boost to ISPs, who will be able to provide ValiCert's Validation Authority Service.

Internet service providers also will have the option of "renting out" ValiCert's technical staff for managing the service. So far, participating ISPs include Frontier Communications Corp., of Rochester, N.Y.; NTT Worldwide Telecommunications Corp., of Tokyo; and Digicert Sdn Bhd, of Kuala Lumpur, Malaysia, said ValiCert officials in Mountain View, Calif.

Certificate revocation has proved to be a roadblock among corporate users, delaying wide distribution of digital certificates and accompanying public-key infrastructures.

Certificate authorities, such as VeriSign Inc., create CRLs (certificate revocation lists), published lists of certificates that have expired (all certificates receive time stamps when they are issued) or have been invalidated because, for example, an employee resigned. VeriSign publishes its revocation list on the Internet in a form that can be accessed by other companies.

But many companies buy certificate server software and take responsibility for managing CRLs in-house and notifying users about which certificates are no longer valid. That has proved to be difficult, hindering cross-company use of certificates.

ValiCert's solution to the problem is something called a certificate revocation tree. This ambitious plan includes creating a worldwide service that ties CRLs together so users-and, most important, IT administrators-have an easier time determining if a certificate is valid.

The Validation Authority supports certificates from Baltimore

Technologies Inc., GlobalSign NV, Entegritty Solutions Corp., GTE Internetworking's Cybertrust, Thawte Certification plc., Entrust Technologies Inc., Microsoft Corp., the Sun-Netscape Alliance and VeriSign.

Some IT managers said the affiliate program, which will double Vali Cert's reach, would make it a lot easier for them to accept certificates from outside the company.

"Having someone manage CRLs would be incredibly useful. Half the time, who knows where (certificates) are coming from?" said Walter Jones, IS director at a Washington-based manufacturing company.

ValiCert can be reached at (650) 254-0170 or www.valicert.com.

COPYRIGHT 1999 Ziff-Davis Publishing Company

COMPANY NAMES: Valicert Inc.--Services
GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Internet service provider; Company service introduction;
Digital signature; Public key encryption
EVENT CODES/NAMES: 366 Services introduction
PRODUCT/INDUSTRY NAMES: 4811522 (Internet Access Providers)
NAICS CODES: 51331 Wired Telecommunications Carriers
FILE SEGMENT: CD File 275

7/9/15 (Item 4 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02259686 SUPPLIER NUMBER: 53555075 (THIS IS THE FULL TEXT)

VALICERT SHIPS DIGITAL CERTIFICATE VALIDATION SUITE.

Computergram International, NA

Jan 12, 1999

ISSN: 0268-716X LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 122 LINE COUNT: 00014

TEXT:

Valicert Inc has upgraded its Enterprise VA Suite, a system for validating digital certificates, to version 2.0. Digital certificates hold the digital keys used to protect information and business transactions in transit across the internet. The Enterprise VA supports a number of validation mechanisms, including certificate revocation lists (CRLs), online certificate status protocol (OCSP), and ValiCert's own certificate revocation tree (CRT). Other components of the suite include standalone and plug-in software modules that check the revocation status of digital certificates; a Validator Toolkit to help developers integrate validation into new and existing applications; and ValiCert's VA Publisher, to distribute CRLs from Microsoft, Netscape and Entrust certificate servers on a regular basis.

COPYRIGHT 1999 ComputerWire Inc.

COMPANY NAMES: Valicert Inc.
GEOGRAPHIC CODES/NAMES: 1USA United States
EVENT CODES/NAMES: 330 Product information
PRODUCT/INDUSTRY NAMES: 7372000 (Computer Software)
SIC CODES: 7372 Prepackaged software
FILE SEGMENT: CD File 275

7/9/16 (Item 5 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02226880 SUPPLIER NUMBER: 21201865 (THIS IS THE FULL TEXT)

Vendors Team On Certificates. (Industry Trend or Event)

Kerstetter, Jim

PC Week, v15, n40, p28(1)

Oct 5, 1998

ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 406 LINE COUNT: 00037

TEXT:

Are digital certificate vendors finally coming in from the cold?

Users hope so, as both Entrust Technologies Inc. and VeriSign Inc.--the leaders in the young digital certificate market--announced late last month that they will both work with security software from Network Associates Inc., of Santa Clara, Calif.

Officials at both companies were quick to point out, however, that the deal was driven by Network Associates' desire to interoperate with as many vendors as possible. They played ball with Network Associates, not with each other.

Still, users are hopeful, and they point to an obvious need for interoperability if PKIs (public-key infrastructures) are to proliferate. "We're considering moving over to a PKI here from our hardware tokens," said a network administrator at a New York bank. "But we're not going to if we're not sure about interoperability. It wouldn't make sense."

That said, the certificate vendors are making it clear that they want--and need--to work with each other more closely. "I have no problem picking up the phone and talking with Stratton (Sclavos, CEO of VeriSign, in Mountain View, Calif.)," said John Ryan, CEO of Entrust, in Richardson, Texas.

Interoperability demo

VeriSign and Entrust recently participated in a certificate interoperability demonstration for banks during the National Automated Clearing House Association's Internet Council CA Interoperability Pilot. It's a mouthful, but it demonstrated that VeriSign and Entrust can work together, along with CertCo Inc. and GTE CyberTrust. IBM's Vault Registry was not involved in the NACHA pilot, but it was built on top of Entrust technology and can interoperate with Entrust certificates.

In the IPsec (IP Security) specification for virtual private networks, VeriSign, Entrust and any companies following IPsec guidelines will have interoperable products. Also under consideration by the Internet Engineering Task Force are two specifications that could lead to interoperability: the PKI Certificate Management Protocol and the Certificate Revocation Syntax.

Add to that mix ValiCert ~~Inc.~~ of Mountain View, Calif., which has a technology called the Certificate Revocation Tree that ties together the Certificate Revocation Lists of certificate authorities, which announce when a digital certificate has been revoked.

Entrust can be reached at (888) 690-2424 or www.entrust.com. VeriSign is at (650) 961-7500 or www.verisign.com. Network Associates is at (408) 988-3832 or www.networkassociates.com. ValiCert is at (650) 567-5400 or www.valicert.com.

COPYRIGHT 1998 Ziff-Davis Publishing Company

COMPANY NAMES: VeriSign Inc.--Contracts; Entrust Technologies Inc.--

Contracts; Network Associates--Products

DESCRIPTORS: Industry Trend; Network Security Software; Computer software industry

PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software)

SIC CODES: 7372 Prepackaged software

FILE SEGMENT: CD File 275

7/9/17 (Item 6 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02180816 SUPPLIER NUMBER: 20736409 (THIS IS THE FULL TEXT)

Digital Certificates Get a Short Lease on Life. (CyberSafe's TrustBroker Public Key Solution to use short-lived digital certificates) (Company Business and Marketing) (Brief Article)

Kerstetter, Jim

PC Week, v15, n21, p33(1)

May 25, 1998

DOCUMENT TYPE: Brief Article

ISSN: 0740-1604

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 557

LINE COUNT: 00047

TEXT:

Users looking for a way around digital certificate revocation problems may have a novel solution from CyberSafe Corp. The Issaquah, Wash., developer will release in the second half of the year its TrustBroker Public Key Solution, code-named Alchemy, whose approach to controlling digital certificates makes them short-lived digital artifacts.

Managing certificate revocation is one area in the Internet community's growing public-key infrastructure that has yet to be fully addressed. Most certificate authorities, such as VeriSign Inc. or GTE Internetworking, rely upon a CRL (certificate revocation list) to let Internet users know when a certificate, used to authenticate a user, has been revoked.

This process works fine as long as everyone involved in the transaction is using the same type of certificate and relying upon the same CA (certificate authority). But once a user ventures into the void between different CAs, there is no automated way to check the validity of a certificate.

Some companies, such as Valicert Inc., have created revocation methods like the Certificate Revocation Tree, which combines various CRLs into a single source.

But CyberSafe is taking a different route with Alchemy. Its Certificate Authority Server, which is part of the TrustBroker Security Server, issues digital certificates that are short-lived. That is, an administrator can set a certificate to last for just a few hours, or up to a day.

Because of this option, a CRL list is not needed. The only way a user can get his certificate renewed is by reconnecting to the server itself, where the administrator has 24-hour-a-day management controls. If the certificate is not renewed, the employee cannot get access to the network.

"Certification revocation has been baffling for me because no one is giving you a straight answer as to how exactly you do it," said Andrew Walski, services administrator at an auto parts supplier in Detroit.

The same applies to outside users in a tight security environment. An outside user, before entering the network, is issued a temporary certificate with the same life-span limits as those used by internal users.

Alchemy also includes the TrustBroker Client, which works in conjunction with the TrustBroker Security Server and the SecretStore database. The VSC (Virtual Smart Card) Option for the client allows a user to store a smart card image and retrieve it at an application launch.

Using the VSC Client option, users don't rely on physical cards but on a digital card that is compliant with PKCS (Public Key Cryptography Standard) 11, for use with Netscape Communications Corp. browsers, or the Microsoft Crypto API standard for Microsoft Corp.'s Internet Explorer browser. Other options include support for key management and key recovery.

CyberSafe will finish beta testing the suite by the end of this quarter. Pricing will be announced when it is released.

CyberSafe is at (425) 391-6000 or www.cybersafe.com.

Certification process

* CyberSafe's TrustBroker Public Key Solution avoids certificate revocation list problems

* Creates a short-lived digital certificate

* Certificate expires in a matter of hours

* Certificates can only be updated by contacting the server

* Users from outside the enterprise are issued a temporary certificate, only after they are qualified by the administrator

COPYRIGHT 1998 Ziff-Davis Publishing Company

COMPANY NAMES: CyberSafe Corp.--Product development

DESCRIPTORS: Company Product Planning; Encryption; Network Security Software

PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software)
SIC CODES: 7372 Prepackaged software
FILE SEGMENT: CD File 275

7/9/18 (Item 7 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02170704 SUPPLIER NUMBER: 20547467 (THIS IS THE FULL TEXT)
VPN Digital Certificate Developers Seek Compatibility, Cooperation. (X.509 Certificate and Certification Revocation List Profile standard)
(Technology Information)
Kerstetter, Jim
PC Week, v15, n17, p20(1)
April 27, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 352 LINE COUNT: 00032

TEXT:

Virtual private networking vendors may be moving forward on IP Security and interoperability, but the digital certificate developers, whose technology provides user authentication for VPNs, are bogged down in the mud of incompatibility.

Users working with digital certificates provided in the public-key infrastructure of Entrust Technologies Inc., for example, cannot automatically check on the validity of a digital certificate issued through VeriSign Inc.'s certificate authority, which is located in Mountain View, Calif.

An Internet Engineering Task Force working group is trying to change that with a recently issued working draft called the X.509 Certificate and CRL (Certification Revocation List) Profile. The draft defines ways for CRLs to interoperate.

"We have to make sure that customers aren't islands on their own when they issue certificates," said Brian O'Higgins, executive vice president and chief technology officer at Entrust, based in Ottawa.

There was a momentary ~~downside~~ to the draft, however, ~~which is based~~ in part on technology developed by Entrust, called the distributed revocation list. The technology, for which Entrust holds a patent and was planning to charge vendors \$50,000 in licensing fees, allows lists to be mirrored on corporate sites throughout the Web.

Entrust officials late last week changed their position and eliminated the fee.

A separate IETF group submitted earlier this month a technology of its own, called OCSP (Online Certificate Status Protocol). OCSP allows a client to automatically check on the status of a certificate.

But OCSP, currently in a six-month review period, is considered a bandwidth hog because it queries the server a second time. Observers question whether it will be widely embraced.

Also, officials of ValiCert Inc., in Palo Alto, Calif., said last week that the company will give away the Version 2.0 of its ValiCert Toolkit.

The new version supports all forms of certificate revocation checking.

ValiCert hopes it will increase interest in its own Certificate Revocation Tree technology, which links the CRLs of disparate certificate authorities so users can go to a single source for certificate verification.

COPYRIGHT 1998 Ziff-Davis Publishing Company

DESCRIPTORS: Technology Development; Virtual Private Network; Standard
PRODUCT/INDUSTRY NAMES: 7372680 (Internet Software)
SIC CODES: 7372 Prepackaged software
FILE SEGMENT: CD File 275

7/9/19 (Item 8 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02142218 SUPPLIER NUMBER: 20301042 (THIS IS THE FULL TEXT)

Warning: is your CRL up-to-date? (managing digital certificates)

(Technology Information)

Kerstetter, Jim

PC Week, v15, n7, p3(1)

Feb 16, 1998

ISSN: 0740-1604

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 740

LINE COUNT: 00063

TEXT:

IT managers planning to deploy digital certificates as part of their public-key architecture should be warned that poorly managed, revoked digital certificates are a potential security threat.

It's such a threat that VeriSign Inc., Microsoft Corp., Netscape Communications Corp., ValiCert Corp., GTE CyberTrust Inc. and Entrust Technologies Inc. are among the vendors scrambling to sign deals with each other to develop technology to ease the management of revoked certificates.

The goal is to develop software that will give corporations immediate access to the lists of certificates--used in public-key exchanges--that have been revoked and, in turn, guarantee that the people with whom they are dealing are authenticated.

Other than expiration dates, there is no current physical means to strip a digital certificate from an invalidated user's computer.

Lexis-Nexis, in Dayton, Ohio, provides digital certificates to law firms throughout the country. These firms, said David Vandagriff, director of technology alliances at Lexis-Nexis, can't afford any lag between the time a certificate is revoked and the time notification is sent to business partners.

"Because confidentiality is so important, the process of making sure people are authorized is critical," Vandagriff said. "I don't want to have to individually tell everyone to get rid of someone's public key in their E-mail."

Current revocation capabilities in applications aren't much better than the little black books merchants once used to check bad credit cards.

For example, VeriSign, of Mountain View, Calif., uses a CRL (Certificate Revocation List), a list of all VeriSign certificates that have been revoked for one reason or another, such as an employee leaving a company. It is displayed on a public Web site and routinely updated to servers at VeriSign customer sites.

As long as the certificate holders on both sides of a transaction are VeriSign customers, the CRL revocation list works fine. But, while VeriSign may be the biggest CA (certificate authority), it isn't the only one.

Most certificate services and software vendors rely on CRLs that don't interoperate. As a result, if a company issues its own digital certificates, it must let others know when one has been revoked.

Does that mean that digital certificates are insecure? Not necessarily. Most digital certificates have an expiration date and can be tied to a responsible CA or a corporation that issues certificates.

Revocation, on the other hand, is a security hole that should concern users.

Many of the security features in the upcoming release of Windows NT 5.0, due later this year, will focus on digital certificates. Microsoft is also working on certificate revocation options.

For starters, the company will ship its new Certificate Server 2.0 certificate management software with Windows NT 5.0 and integrate it with Windows NT's Active Directory, said Karan Khanna, product manager at Microsoft, in Redmond, Wash.

With that integration, Windows NT 5.0 will gain a CRL list. Microsoft's Internet Explorer 4.0 supports the company's existing Authenticode certificate revocation capabilities, though in default mode this capability is turned off. Internet Explorer will support CRLs later

this year.

Netscape's Communicator client currently has limited support for revocation checking, though officials in Mountain View, Calif., say the company will improve CRL support in Navigator and Communicator by year's end.

On the server side, Netscape's Certificate Server currently supports CRLs and integrates them with Lightweight Directory Access Protocol directories.

VeriSign and other vendors are also working on the proposed OCSP (Online Certificate Status Protocol), which will allow an automatic check on a certificate's status.

However, the specification, under development by the Internet Engineering Task Force, is still months from completion. There also is concern that OCSP could be a bandwidth hog, since it establishes a second connection back to the server to check on a certificate's status.

For its part, ValiCert, of Sunnyvale, Calif., has created a certificate revocation tree, which would allow CRLs to interoperate, and has licensed its tool kit to GTE, Netscape, Entrust and others. Next quarter, GTE will release a tool kit that will allow its corporate customers to check the CRL listings.

IT departments, users say, should be cautious as they extend certificate services across the Internet. "A security breach," said Vandagriff, "always comes at the borders of technology."

COPYRIGHT 1998 Ziff-Davis Publishing Company

DESCRIPTORS: Technology Application; Internet Security; Data Security
Issue; Public Key Encryption

PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software)

SIC CODES: 7372 Prepackaged software

FILE SEGMENT: CD File 275

7/9/20 (Item 9 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)

(c) 2002 The Gale Group. All rts. reserv.

02111797 SUPPLIER NUMBER: 19909029 (THIS IS THE FULL TEXT)

Easing management of digital certificates. (NetDox's DoxIt digital certificate management service; ValiCert's ValiCert Toolkit and ValiCert Server digital certificate management software) (Company Business and Marketing)

Kerstetter, Jim

PC Week, v14, n44, p10(1)

Oct 20, 1997

ISSN: 0740-1604

LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 502

LINE COUNT: 00044

ABSTRACT: NetDox and ValiCert are readying new digital certificate management software products and services geared at providing companies with improved security controls. NetDox plans to introduce its DoxIt certificate management service during the week of Oct 20, 1997. The service, priced at \$5.35 per transaction, places the company between users and their e-mail. NetDox's service insures message integrity for up to \$50,000 and the company uses double encryption technology to escape encryption export issues. For its part, ValiCert plans to release its \$995 ValiCert Toolkit and ValiCert Server. The tool kit promises to enable developers to integrate digital certificate validity monitoring that is compliant with the X.509 certificate standard. The ValiCert Server, priced on configuration, allows administrators to develop certificate revocation trees that automatically determine certificate validity.

TEXT:

Two small companies this week will try to fill what they believe is a void in digital certificate management with new software and services that

give companies improved control over security.

NetDox, of Deerfield, Ill., will unveil a new certificate management service called DoxIt. With the service, the company acts as an intermediary between users and their E-mail.

NetDox doesn't want to be a certificate authority or create certificate management software. Instead, it wants to create a service business, with pricing starting at \$5.35 per transaction, that ensures both the integrity and interoperability of the certificates.

The sender uses a free NetDox GUI to determine recipients, package and encrypt the document, and send it to the NetDox Processing Center in Illinois.

The Processing Center, in turn, authenticates the sender, identifies the receiver, verifies the integrity of the message contents and creates an audit trail for the message. The recipient decrypts the message and automatically sends out a confirmation receipt.

NetDox will insure the integrity of each message for up to \$50,000, said Thomas Friedman, vice chairman of the company.

NetDox uses a double encryption technique to allow it to get around encryption export issues. Each message essentially has two wrappers. The inner wrapper uses 40-bit RSA Data Security Inc. public key encryption--exportable under current law without many restrictions. The outer wrapper is 128 bits--significantly stronger encryption that has yet to be broken, but is illegal to export from the United States.

But NetDox has worked out a deal with the government that will allow it to export the strong encryption: If issued a warrant, it will provide government investigators with a way through the outer wrapper, Friedman said.

The Boston law firm of Hale and Dorr just finished piloting the NetDox service and found that it answered critical privacy concerns for a law firm passing information over the Internet.

"We found that existing encryption protocols were very difficult to work with and that we weren't getting a return receipt requested," said senior partner Ken Slade. "We found that NetDox answered both those concerns."

Early next year, NetDox will start a certificate mediation service that will grade the trustworthiness of certificates, whether they are generated by a certificate authority such as VeriSign Inc. or by a corporation internally.

Separately, ValiCert, a Sunnyvale, Calif., startup, will release this week the ValiCert Toolkit and ValiCert Server.

The tool kit, priced at \$995 per year, will enable developers of other applications--including Web browsers, virtual private networks, electronic data interchange and payment systems--to integrate validity checking for digital certificates that are compliant with the X.509 certificate standard.

ValiCert Server enables administrators to construct a "certificate revocation tree" to automatically determine when a certificate is invalid. Pricing will vary, depending on configuration.

DoxIt ensures the integrity of digital certificates for \$5.35 a transaction.

COPYRIGHT 1997 Ziff-Davis Publishing Company

SPECIAL FEATURES: other; illustration

COMPANY NAMES: NetDox Inc.--Services; Valicert Inc.--Product introduction

DESCRIPTORS: Company Service Introduction; Company Product Planning;

Network Security Software

PRODUCT/INDUSTRY NAMES: 4811500 (Specialized Telecommunication Services); 7372613 (Network Security Software)

SIC CODES: 4822 Telegraph & other communications; 7372 Prepackaged software

TRADE NAMES: ValiCert Toolkit (Network security software)--Product introduction

FILE SEGMENT: CD File 275

7/9/21 (Item 1 from file: 647)

DIALOG(R) File 647: CMP Computer Fulltext
(c) 2002 CMP Media, LLC. All rts. reserv.

01142885 CMP ACCESSION NUMBER: INW19971027S0074

Managing Digital Certificates - ValiCert unveils product, service suite

Rutrell Yasin

INTERNETWEEK, 1997, n 687, PG52

PUBLICATION DATE: 971027

JOURNAL CODE: INW LANGUAGE: English

RECORD TYPE: Fulltext

SECTION HEADING: Management & Security

WORD COUNT: 382

TEXT:

By the year 2000, there will be millions of digital certificates in use. With that prediction in mind, users and vendors have begun to wonder how they are going to manage them all.

Getting a jump on the pack of vendors that hope to capture the certificate-management market, start-up ValiCert Inc. last week rolled out a suite of products and services designed to solve the certificate-revocation problem.

The ValiCert Toolkit, ValiCert Server and ValiCert Services will give users a way to distinguish between valid and compromised X.509 digital certificates in real time, according to Joseph "Yossi" Amram, ValiCert president and CEO.

Certificates-encrypted electronic signatures that bind a person's or a company's identity to a message or transaction-are an important component for security in transacting business over the Internet or corporate intranets.

Currently, security systems validate certificates by checking them against electronic lists of "bad numbers," known as certificate-revocation lists (CRLs). To verify a certificate, an administrator must obtain the latest list and then use memory-sapping software to sift through the list and ensure that the certificate in question is not on the list.

As the public key infrastructure grows, the number of certificates will expand beyond current systems, according to Michael Goulde, a senior analyst with the Patricia Seybold Group.

"As revocation lists get bigger and bigger, the present system is not going to work," Goulde said.

Anticipating a need for a more efficient way to validate certificates, ValiCert launched a "revocation tree" that delegates the job of list checking, Goulde said. This approach makes it easier to identify bad number information contained in multiple CRLs, he said.

Software developers can use the ValiCert Toolkit to embed certificate-validation capabilities into their user applications, ValiCert said.

ValiCert also launched the ValiCert Server, which builds a certificate revocation tree from a certificate revocation list.

ValiCert Services will act as a clearinghouse for checking the validity of certificates. Any application that uses ValiCert technology will be able to request verification of digital certificates from ValiCert servers, according to ValiCert officials.

The tool kit and server are available now; ValiCert Services will ship in the first quarter of 1998. The tool kit costs \$995. The server costs \$9,995 and supports Windows NT and Sun Solaris systems.

Copyright (c) 1997 CMP Media Inc.

COMPANY NAMES (DIALOG GENERATED): Patricia Seybold Group ; ValiCert Inc ;
ValiCert Services

7/9/22 (Item 2 from file: 647)

DIALOG(R) File 647: CMP Computer Fulltext
(c) 2002 CMP Media, LLC. All rts. reserv.

01141583 CMP ACCESSION NUMBER: CRN19971020S0034

Encryption Start-Up Serves Servers

Charlotte Dunlap

COMPUTER RESELLER NEWS, 1997, n 759, PG24

PUBLICATION DATE: 971020

JOURNAL CODE: CRN LANGUAGE: English

RECORD TYPE: Fulltext

SECTION HEADING: News

WORD COUNT: 273

TEXT:

Sunnyvale, Calif. - A new encryption start-up, launching today, aims to provide a service that verifies the validity of digital certificates in realtime and offer toolkits and servers to VARs.

Staffed with a "Who's Who" of cryptography, ValiCert Inc., based here, will sell its toolkits to developers of commerce systems for added security. It also has signed deals with vendors, including Netscape Communications Corp., to embed ValiCert's encryption server technology into the vendors' servers. And finally, the company will provide a service to anyone involved in communicating via digital certificates, to immediately determine the validity of X.509 digital certificates.

"The core of our technology is the mathematical and cryptographic data infrastructure, called a certificate revocation tree," said Chini Krishnan, chairman, chief technology officer and founder of the company.

The technology securely transfers updated information regarding digital certificates to every computer on its server. ValiCert's technology is able to differentiate between valid and compromised digital certificates, he said.

Digital certificates are encrypted electronic "signatures" that attach the identification of a person or company to their electronic message or transaction.

Also on the ValiCert team are Paul Kocher, co-founder and chief scientist, who designed the cryptography for Netscape's current security technology, Secure Sockets Layer; and Marty Hellman, the co-inventor of public key cryptography, known as Diffie-Hellman.

The ValiCert Toolkit will be offered to VARs and software developers for an annual licensing fee of \$995.

Vendors, including Netscape will release a plug-in for the technology in future versions of its SuiteSpot servers. ValiCert initially will conduct field trials of its verification service, with broad availability slated for 1998.

Copyright (c) 1997 CMP Media Inc.

COMPANY NAMES (DIALOG GENERATED): Netscape Communications Corp ; ValiCert Inc.

7/9/23 (Item 1 from file: 674)

DIALOG(R)File 674:Computer News Fulltext

(c) 2001 IDG Communications..All rts.. reserv.

080086

ValiCert launches online validation authority service for digital certificates

Byline: Ellen Messmer

Journal: Network World

Publication Date: December 08, 1999

Word Count: 298 Line Count: 30

Text:

]ValiCert this week will launch one of the first online digital certificate validation services that supports multivendor security certificates, including those from Thwate, Entrust, GTE, VeriSign and Baltimore Technologies.]Each public-key digital certificate, regardless of what organization issues it, needs to undergo a validation check each time the key is going to be used to ensure it hasn't expired or been revoked. This is done by means of a validation server, but unfortunately, there is little uniformity so far in how the public-key infrastructure (PKI) vendors want this done.ValiCert has stepped in with a service that lets

organizations that deploy multiple certificates outsource the validation task for a fee starting at \$30,000 per year. The ValiCert service supports the multiple PKI protocols, including the Online Certificate Status Checking Protocol, CRL distribution, and certificate revocation trees. "The U.S. Navy and Netscape are validating certificates using our services," says Josi Amram, CEO of ValiCert. Outsourcing certificate validation is hardly a trivial security decision since ValiCert is put in charge of the certificate's private keys. If an intruder grabbed them, certificates would be compromised. If the validation service went down, the user's certificate wouldn't be available for use in authentication, signing and encryption. To gain customer trust, Amram says that ValiCert's data facility here is heavily secured with back-up capabilities. Employees authenticate their identity to ValiCert's internal network by means of security procedures that include retinal scan and biometric authentication. Besides the convenience of having one service validate different vendor certificate types, ValiCert makes the argument that outsourcing the task to a third party such as itself is a good decision. "It's separation of duties between the vendor that issued the certificate and the validation function," Amram asserts. This separation adds an independent source to make sure certificates are being properly issued and revoked.

7/9/24 (Item 2 from file: 674)

DIALOG(R) File 674:Computer News Fulltext

(c) 2001 IDG Communications. All rts. reserv.

062698

ValiCert makes offer to track digital deadbeats

Certificate revocation system requires buy-in from electronic-commerce community

Byline: Sharon Machlis

Journal: Computerworld Page Number: 20

Publication Date: October 20, 1997

Word Count: 393 Line Count: 38

Section Heading: News

Text:

A cryptography start-up says it's got the solution for what is likely to become a sticky problem in managing digital certificates: how to handle certificates that go bad.

Much like with credit cards in the physical world, issuers and users of digital certificates must ensure that those certificates used to confirm payments or authorize transactions are actually valid.

If a certificate is lost (such as when a laptop is stolen) or revoked (if its owner doesn't pay the bill), the issuing authority must somehow notify vendors throughout cyberspace.

The emerging electronic-commerce structure would rely on certificate revocation lists (CRL), files similar to lists of bad credit cards. But the founders of ValiCert, Inc. said as electronic commerce becomes more popular and the number of digital certificates mushrooms, the CRLs will become too large and unwieldy for quick real-time transactions.

ValiCert's answer involves collecting CRLs from various certificate issuers and using an algorithm to create certificate revocation "trees." By tagging each certificate on the list to various levels of information above it, the amount of data is streamlined by pointing to the location on the tree instead of incorporating the full data.

Cryptography expert Martin Hellman is on the company's advisory board and said ValiCert's technology addresses an important roadblock to certificate validation.

But for the ValiCert technique to work, it must be incorporated in various electronic-commerce applications, all major certificate issuing authorities must adopt it, and electronic-commerce vendors must choose to turn to ValiCert for checking on certificates.

"They've definitely made the right partnerships," said Marlo Kosanovich, a senior research analyst at Meta Group, Inc. in Stamford, Conn. "Whether it works or not remains to be seen." It depends on whether

the company's tool kit is used to implement real-world applications for the concept, she added.

INDUSTRY SUPPORT

Several major players support the concept, including Entrust Technologies Ltd. in Richardson, Texas, and GTE CyberTrust in Needham, Mass.

The ValiCert tool kit is available free for noncommercial use and evaluation at www.valicert.com. Application development licenses cost \$995 per year. A ValiCert server will be licensed to certificate issuing authorities.

Kosanovich predicted it will be late 1998 before the use of digital certificates begins to take off. "They're off to what seems to be a promising start," she said of ValiCert. Now the company has to wait as the market catches up, she added.

7/9/25 (Item 1 from file: 696)

DIALOG(R) File 696:DIALOG Telecom. Newsletters
(c) 2002 The Dialog Corp. All rts. reserv.

00601385

VENDOR GIVES AWAY TOOL KIT FOR CERTIFICATE VERIFICATION

ELECTRONIC COMMERCE NEWS

April 27, 1998 VOL: 3 ISSUE: 17 DOCUMENT TYPE: NEWSLETTER

PUBLISHER: PHILLIPS BUSINESS INFORMATION

LANGUAGE: ENGLISH

WORD COUNT: 280

RECORD TYPE: FULLTEXT

TEXT:

ValiCert Inc. is offering the newly-upgraded version of its digital certificate authentication tool kit free on its World Wide Web site.

The Palo Alto, Calif.-based developer has enhanced its ValiCert Tool Kit to support multiple validation and revocation protocols. The company says this makes its software a universal validation product.

"Digital certificates are becoming the method by which you identify someone [in EC environments]," says ValiCert CEO Yosi Amram.

"But most products don't do revocation checking. The certificate could have been revoked but there is no mechanism in the browser to check the validity."

Version 2.0 of the tool kit gives developers of electronic commerce applications the software components necessary for their systems to validate certificates. Developers may use authentication mechanisms such as certificate revocation lists and online certificate status protocol.

Trumpeting A Universal Solution

The older version of ValiCert's tool kit cost \$1,000 and only used the company's proprietary validation mechanism, called certificate revocation trees.

The company will now rely on its other software and services to generate sales revenues, Amram says. The company sells software that issues certificate validations for organizations using certificates for internal firewall access control. It also offers services to secure EDI communication between organizations.

"ValiCert's support of multiple validation and certificate revocation protocols demonstrates the true interoperability that is crucial for the global adoption of electronic commerce for the banking and financial services industry," says Adam Backenroth, president of the Chicago-based Financial Services Technology Consortium, a nonprofit organization that develops interbank technical projects to improve the competitiveness of the financial services industry.

(Yosi Amram, ValiCert Inc., 650/849-9860,

http://www.valicert.com; Adam Backenroth, Financial Services
Technology Consortium, 312/527-6724, http://www.fstc.org.)

(c) PHILLIPS PUBLISHING INTERNATIONAL All Rts. Reserv.

COMPANY NAME(S): EDI ; Financial Services Technology Consortium ; ValiCert
Inc ; Yosi Amram

7/9/26 (Item 1 from file: 9)

DIALOG(R)File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

02614061 (THIS IS THE FULLTEXT)

Valicert System No Longer a Niche Product

**(Valicert and its validation technology for digital certificates are
gaining more prestige)**

American Banker, v 164, n 208, p 22

October 28, 1999

DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 1064

ABSTRACT:

Valicert Inc, as well as its validation technology for digital certificates
are not being demoted to technically obscure roles anymore in electronic
commerce security.

What Valicert dubs its third-generation Enterprise VA Suite 3.0 gets much
deeper into business operations than just determining that a digital
credential has not expired or been revoked -- the fundamental definition of
certificate validation.

The Mountain View, Calif., company has just begun shipping the most recent
version of its validation authority, or VA, system. With the announcement
came a number of indications that the company's notion of validation,
somewhat of a difficult sell when it was new and not widely understood, is
finding a place in the quickly evolving Internet security infrastructure.

TEXT:

By JEFFREY KUTLER

Valicert Inc. and its validation technology for digital certificates are no
longer being relegated to technically obscure roles in electronic commerce
security.

The Mountain View, Calif., company has just begun shipping the latest
version of its validation authority, or VA, system. With the announcement
came several indications that the company's notion of validation, something
of a tough sell when it was new and not widely understood, is finding a
place in the quickly evolving Internet security infrastructure.

What Valicert calls its third-generation Enterprise VA Suite 3.0 gets much
deeper into business practices than just ascertaining that a digital
credential has not expired or been revoked -- the basic definition of
certificate validation.

The package has several "application level" features that go to the heart
of what banks and other companies want to be doing on the World Wide Web.
And in a tangible sign of business progress by Valicert, its technology is
being incorporated in significant e-commerce efforts such as the Identrus
multinational banking consortium, the U.S. government's ACES -- Access
Certificates for Electronic Services -- project, and various aspects of the
Sun-Netscape Alliance, which is an e-commerce venture of Sun Microsystems
Inc. and America Online Inc.'s Netscape Communications subsidiary.

Officials of Valicert, which in September raised \$23 million in mezzanine-stage financing from an international group led by Lucent Venture Partners, say three years of hard work in system development and market education are paying off.

Also in September, the company announced the opening of a European headquarters in Amsterdam, which president and chief executive officer Yosi Amram termed "another step in our mission to build a global validation network for secure e-commerce."

The digital certificates that many banks, government entities, and other "trusted third parties" view as a key to authenticating on-line trading partners will have to go through a validation step, the reasoning goes. "The coming explosion in business-to-business transactions" will need this "critical enabler," said Valicert vice president of marketing and business development Sathvik Krishnamurthy. "Only Valicert is offering a complete, proven solution."

Among those sending kudos Valicert's way was Scott Lowry, president and CEO of Digital Signature Trust Co., a subsidiary of Zions Bancorp. of Salt Lake City and one of the first two vendors selected to provide the data encryption backbone for the government's ACES program.

Valicert's Enterprise VA Suite will be a part of the public key infrastructure systems of both Digital Signature Trust and the other approved ACES vendor, Operational Research Consultants Inc.

"With its third-generation product," Mr. Lowry said, "Valicert has shown the ability to provide the robust validation capabilities that may be required by a project of such magnitude as ACES." The program sets a standard for management of digital certificates to ensure secure communications between citizens and the government.

Daniel E. Turissini, vice president of Operational Research Consultants, said, "Because of the multivendor nature of this project, it is crucial to have universal validation services, and Valicert is the perfect solution."

The validation vendor is not alone in offering this service. Certco Inc. of New York recently added a validation component based on the OCSP -- On-line Certificate Status Protocol -- to its digital trust technology offering.

But Valicert has attempted to set a standard for flexibility and compatibility. It worked to make its VA interoperable with all major providers of certificate authority, or CA, systems, among them Baltimore Technologies, Entrust, GTE Cybertrust, Thawte, and Verisign.

"We are viewed as a trusted third party, neutral, because we are not competing as a CA," said Ram Krishnan, Valicert's director of product marketing.

David Ferris, president of Ferris Research, a San Francisco-based firm focusing on messaging technologies, said, "This is an important niche, dominated by one vendor, Valicert. It's strange the firm doesn't have any real competition."

Valicert's VA "provides a clearing-house function for users of digital-certificate-based applications," said Eric Hemmendinger, senior analyst at Aberdeen Group of Boston. "Automatically confirming the validity of digital certificates issued by multiple suppliers' CAs, the VA provides a valuable form of insurance critical for enterprises conducting e-business."

Mr. Krishnan said the company is also "agnostic" when it comes to technical protocols for validation. It will support CRL, or Certificate Revocation Lists; the CRL-Distribution Points variation; OCSP; and Certificate

Revocation Trees, a Valicert invention.

"The mission always has been to validate any certificate, from any CA, any protocol, anywhere on the planet," Mr. Krishnan said. "It is tough to make that claim. We are backing it up."

Valicert is billing Enterprise VA Suite 3.0 as "the first complete, universal certificate validation solution."

Among the enhancements to one of the components, the server system that has been on the market two years, is a mechanism called Stateful Validation. Going beyond simple certificate verification, it enables validation of "things specific to the application's context," Mr. Krishnan said. In other words, the system can verify an aspect of a transaction other than a credential's validity, inquiring into a credit bureau or human resources data base, for example.

Valicert has described its validation function as equivalent to a credit card authorization. Mr. Krishnan extended the analogy for Stateful Validation: "It tells you not only that the credit card is good, but that the customer is authorized to buy \$5,000 of stuff."

Enterprise VA 3.0 has been enhanced to serve networks of certificate authorities operating in multiple locations, such as Identrus. Banks will be both competing with each other and cooperating to obtain validations, which the Valicert framework can accommodate.

There is also a feature called Enterprise VA Mirroring, which enables data to be replicated or shared efficiently among several validation authorities that may be scattered around the world.

Such capabilities add up to "more integration (of VA) with business applications," Mr. Krishnan said. "The power of what we do is only as good as the applications we are supporting," and they range from Web servers and browser software to virtual private networks and secure e-mail.

"Customers really seem to be excited," Mr. Krishnan added. He said Valicert's selection for the forthcoming Identrus pilot and its signing of one of that consortium's founding banks, ABN Amro, will be followed by more banking industry contract announcements.

"We are feeling good that our message is getting out to the financial services industry," Mr. Krishnan said. "It is critically important to secure what they do, and they realize that their certificate technology is incomplete without validation."

Copyright 1999 Thomson Information Services Inc.

COMPANY NAMES: VALICERT INC

INDUSTRY NAMES: Software

PRODUCT NAMES: Utility software packages (737242)

CONCEPT TERMS: All product and service information; Product introduction

GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/27 (Item 2 from file: 9)

DIALOG(R) File: 9:Business & Industry(R)

(c) 2002 Resp.: DB Svcs.. All rts..reserv.

02572978 (THIS IS THE FULLTEXT)

Data Security Firm Adds Validation Function

(Certco Inc introduced CertValidator, a system that assures the validity of a digital certificate presented in an electronic commerce transaction)

American Banker, v 164, n 178, p 14

September 16, 1999

DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1098

ABSTRACT:

Certco Inc introduced CertValidator, a system that assures the validity of a digital certificate presented in an electronic commerce transaction. In efforts to complete Internet commerce infrastructure construction, certificate validation has become an important issue. CertValidator is build on online certificate status protocol (OCSP), the leading alternative to certificate revocation list (CRL). Firms that sell digital certificate and public key encryption technologies have made efforts to deal with non-CRL options such as OCSP. Valicert Inc, a validation technology supplier, has heightened awareness of OCSP with its own product and its own technology. Valicert has been awarded \$23 mil in a mezzanine round of venture capital financing. Valicert's financing and the development of OCSP are discussed.

TEXT:

By JEFFREY KUTLER

Certco Inc. has added a powerful validation component to its digital trust technology.

The New York data security company, a spinoff of the former Bankers Trust Corp., introduced CertValidator, a system that assures the validity of a digital certificate presented in an electronic commerce transaction.

Certificate validation has become a critical issue -- for some, a stumbling-block -- in attempts to complete the construction of Internet commerce infrastructures.

In the digital equivalent of the printed credit card "hot lists" of the 1960s and 1970s, an on-line seller might have to consult an unwieldy certificate revocation list, or CRL, to see if a presented credential expired or was revoked. CRLs are widely considered unworkable for large-volume networks that put a premium on speed. A leading alternative is OCSP -- the on-line certificate status protocol -- on which CertValidator is built.

Vendors of public key encryption and digital certificate technologies have taken steps to accommodate non-CRL options like OCSP. Xcert International Inc. of Walnut Creek, Calif., has explicitly avoided CRLs because it views on-line, real-time status checking as essential. One company specializing in validation methods and related support services, Valicert Inc. of Mountain View, Calif., has raised consciousness about the issue with its own technology, certificate revocation trees, as well as OCSP.

Certco differs from Valicert's Validation Authority offering, said Certco senior vice president Jay Simmons, in that it integrates a secure OCSP data repository with the "responder" function.

Yosi Amram, president of Valicert, said, "I and Valicert welcome the entry of Certco into the validation space.

"This helps to further legitimize the business need" and reinforces "a message that Valicert has been conveying to the market for over two years."

Calling CertValidator "the second leg of a product offering" that began with certificate authority systems, Mr. Simmons said, "We believe it will be necessary to know who issued a certificate and to get a positive response that it has been issued."

Among the key benefits would be nonrepudiation. A buyer of goods, for example, would be unable to claim improperly or fraudulently after the fact

that the transaction did not occur.

In keeping with open interoperability principles, CertValidator can store and manage certificates, CRLs, and status data from all major certificate authority vendors. The president of one of them, Peter Hussey of GTE Corp.'s Cybertrust unit, said the program fits well with its "secure extranet" offerings. "This powerful technology not only gives our customers a flexible option for accelerating their business-to-business e-commerce activities," Mr. Hussey said, "but it also makes them more secure."

"Real-time validation capability within and across public key infrastructures is critical for businesses that intend to engage in high-value e-business transactions via the Internet," said Diana Kelley, senior security analyst with Hurwitz Group Inc. "OCSP support and multivendor interoperability are features that the market should demand." Richard Salz, the architect of CertValidator, said the system's foundations in standards such as OCSP and LDAP (lightweight directory access protocol) and certification for meeting high-level Federal Information Processing Standards contribute to the all-important flexibility and scalability requirements sought by customers.

Included on a long list of CertValidator operational features are hardware-based data encryption and key storage, tamper-proofing, audit trails, and two trademarked ideas, Fast-Path Revocation and Fast-Path Suspension. The former occurs much faster than the hours or days that a CRL system might take. With the latter, a hold can be placed on a certificate in a critical situation, then quickly lifted to return it to valid status.

Meridien Research senior analyst Octavio Marenzi said OCSP responders and repositories can meet the instantaneous information needs of trading partners only if they are "highly secure, fully interoperable, and scalable. All (those) characteristics appear to be present" in CertValidator.

Certco president and chief executive officer John Herron said CertValidator is an "industrial-strength implementation of OCSP," resulting from the company's mix of skills in such areas as cryptography, banking, law, software, and risk management.

"Many of our technical advantages are simple in design yet sophisticated in concept, the product of engineers and others who know a lot more than just technology," Mr. Herron said.

Mr. Simmons said the system is not only designed "as a secure repository for managing certificate life cycles across multiple certificate authorities," but also is well suited for "the Identrus model" -- a certificate infrastructure that requires multiple participating banks to be in sync with validation.

Certco, in fact, was instrumental in the formation last year of Identrus LLC, a multinational business-to-business trust consortium that included among the founders Bankers Trust and its Germany-based acquirer, Deutsche Bank.

Mr. Simmons said he views Identrus as one of the likely sparks to growth in commercial use of public key encryption technologies in the coming year. "Y2K will be behind us, and we see the banks moving very aggressively," he said.

Certco relinquished its shareholder position in Identrus to compete on an even footing for the banks' business. A rival, Baltimore Technologies, was designated root-key supplier for the pilot phase, and Valicert won a role for its validation tools.

Mr. Amram described CertValidator as "effectively an OCSP responder product," whereas his company, Valicert, is already into a "third

generation" with a multipronged strategy including a server that supports all protocols and a third-party validation authority service.

"OCSP is a key component of Identrus' risk management strategy," said the consortium's chief operations and technology officer, Kristin Kupres. "It's great to see Certco respond to the need for real-time digital certificate validation by advancing this important standard."

MOUNTAIN VIEW, Calif. -- The Validation technology supplier Valicert Inc. said it has obtained \$23 million in a mezzanine round of venture capital financing.

Leading the investment group was Lucent Venture Partners, an arm of Lucent Technologies. Other members included Canadian Imperial Bank of Commerce, Financial Technology Ventures, First Analysis, France Telecom, Gemplus, Korea Technology Banking, Mitsui, and Thomson-CSF Ventures.

This money came on top of \$7 million last year from August Capital, Bessemer Venture Partners, Draper Fisher Jurvetson, Intel, and U.S. Venture Partners, all of which were also in the mezzanine round.

"This round of funding will enable Valicert to greatly extend the availability of its Validation Authority solutions, allowing companies around the world to securely conduct business transactions over the Internet," said Jean-Michel Barbier, president of Thomson-CSF Ventures, the investment unit of the French technology company.

Valicert president and chief executive officer Yosi Amram said he is "excited at the breadth and diversity of our new investor syndicate. We expect their financial, technology, and distribution experience to play a critical role as we continue to add value to our business."

Copyright 1999 Thomson Information Services Inc.

COMPANY NAMES: CERTCO LLC
INDUSTRY NAMES: Information industry; Online services
PRODUCT NAMES: On-line service providers (737500)
CONCEPT TERMS: All market information; All product and service information
; Product introduction; Trends
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/28 (Item 3 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

02488504 (THIS IS THE FULLTEXT)
On-Line Banking: Valicert Adds Allies to Rule the Validation World
(Valicert enters licensing and distribution agreements with Equifax Secure and IBM for its digital certificate validation systems)
American Banker, v 164, n 115, p 12
June 17, 1999
DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 986

ABSTRACT:
Valicert Inc (Mountain View, CA) has entered recent deals with Equifax Secure Inc and International Business Machines Corp (IBM). These alliances add on to previous alliances with a number of leading vendors operating in the area of digital certificates. Valicert offers certificate validation technology-systems that can determine if a digital certificate has expired or been revoked. With the new deal with Equifax Secure, Valicert's

Enterprise VA Suite 2.0 has been licensed to offer to customers of the Equifax Secure e-commerce security program. Equifax Inc (Atlanta), meanwhile will become a reseller of Valicert's VA validation authority system. The IBM deal makes IBM's VaultRegistry certificate-issuance system compatible with Valicert products. Other Valicert partners include Baltimore Technologies, Digital Signature Trust Co, Entrust Technologies and Celo Communications. Full text discusses Valicert products, Valicert alliances, and digital certificate technology.

TEXT:

By JEFFREY KUTLER

Valicert Inc., which is trying to lock up one of the specialty markets associated with electronic commerce security, continues to lengthen its list of strategic allies.

The three-year-old company announced agreements last week with Equifax Secure Inc. and International Business Machines Corp., which itself is a close ally of Equifax Inc.'s digital security offshoot.

On top of a series of other cooperation and distribution agreements in recent months, the latest alliances solidify Valicert's claim to serving as the premier source of certificate validation technology-systems that can be used to verify that a digital certificate has not expired or been revoked.

Most leading vendors of public key infrastructures for digital certificates-including Entrust Technologies Inc., Verisign Inc., Baltimore Technologies PLC, GTE Corp.'s Cybertrust unit, Celo Communications of Sweden, and Thawte Certification-have some form of system-integration or interoperability agreement with Valicert.

In a business rife with strategic alliances because few if any companies can deliver the complete range of data security components by themselves, Valicert's record of cooperation is as extensive as any.

Equifax Secure, for example, licensed Valicert's Enterprise VA Suite 2.0 and will make it available to customers of its e-commerce security program. The division of Atlanta-based Equifax Inc., a leader in the consumer information and credit reporting industries, will also serve as a reseller of Valicert's VA, or validation authority, system.

IBM made its VaultRegistry certificate-issuance system, which is a key element of Equifax Secure's offering, compatible with Valicert products such as Enterprise VA and the Valicert Global VA Service.

By incorporating the Valicert technology, "IBM is able to support a wider range of e-business applications as it provides enterprises with trust around the globe," said Mark Greene, the computer giant's vice president of security.

"Valicert is a recognized leader in providing complete and efficient validation authority solutions for digital certificates," said Equifax Secure general manager Jeffrey Johnson. "We look forward to expanding the scope of our certificate issuance systems"-customers will have the option of acting as their own validation authorities rather than relying on an outside service.

Valicert aims to resolve one of the thorny complications of digital certificate operations. Validation of certificates in public key encryption infrastructures, or PKIs, can be so difficult or inefficient that some security-technology innovators have proposed alternative approaches that do without validation per se.

But PKI methods are well entrenched and gaining new adherents as e-commerce takes hold. Encryption keys for digital certificates, the

credentials that banks or other trusted parties issue to vouch for a customer's on-line identity, are standard equipment in Internet browser software, for example. (Browser leaders Microsoft and Netscape are on Valicert's partner list; Microsoft's Internet Explorer 5 has validation built in.) Certificates are required of banks, merchants, and consumers by SET, the Secure Electronic Transaction protocol for Internet credit card payments.

PKI proponents like Mr. Greene of IBM acknowledge that it could take years for these technologies to get fully established. But Mr. Greene pointed out in a recent interview that "it is possible to get it to work without exposing users to all the complexity."

As long as there are PKIs, validation will be an issue-and it is one of the areas where ingenuity is being applied to reduce the operational burdens.

Valicert itself has adjusted to market demands. The Mountain View, Calif., company initially came on the scene with a validation method called Certificate Revocation Tree, considered a vast improvement over the cumbersome checking of certificate revocation lists, or CRLs. Valicert president and chief executive officer Yosi Amram likened CRLs to the paper "hot card bulletins" that retailers had to consult in the early days of credit cards.

In assembling its validation capabilities, however, Valicert recognized that its revocation trees would not displace CRLs overnight. Meanwhile, a new technique called OCSP-On-line Certificate Status Protocol-gained ground within the Internet Engineering Task Force's standards-setting program. To offer complete coverage, Valicert therefore supports CRL and OCSP.

"By working with Valicert, IBM has expanded the options its global customers have to implement a comprehensive, security-rich solution for engaging in communications and commerce over the Internet," Mr. Amram said last week. "We expect additional companies to rely on IBM and Valicert technology to expand the availability of global validation and intend to continue to work closely with IBM to ensure that our products interoperate effectively to enable world-class solutions for enabling global e-business."

Though Valicert had been cooperating at some level with PKI companies almost since its inception, recent announcements took on deeper significance. In March, Thawte of South Africa and GlobalSign of Belgium, which had been testing the validation systems, embarked on more formal integration and distribution arrangements.

Baltimore, a British-Irish PKI leader that participated in the March announcement with a licensing and distribution pact, announced a more comprehensive technology integration on April 27. Citing Valicert's OCSP support, Baltimore marketing vice president Patrick Holahan said the deal "adds an enhanced level of trust to Baltimore Unicert digital certificates."

Also in April, Entrust Technologies of Plano, Tex., joined in a "validation interoperability" announcement, encompassing both the Entrust- championed CRL Distribution Points methodology and OCSP.

"Our partnership with Valicert brings additional revocation choices to our PKI customers through either CRLDP or OCSP standard formats," said Entrust CEO John Ryan.

In mid-April, Digital Signature Trust Co., a subsidiary of Zions First National Bank of Salt Lake City, said it would add the Valicert VA to its certificate repository architecture.

The repository is "the central point of trust for our customers," said

Digital Signature Trust president Scott Lowry. He said the Valicert technology would "increase interoperability and improve the performance of our repository certificate-validation queries."

A Sampling of Valicert Partners
Baltimore Technologies

Unicert certificates get validation capability

Digital Signature Trust Co.

Valicert components in certificate repository

IBM

VaultRegistry compatible with Valicert software

Entrust Technologies

Valicert system provides new revocation option

Equifax Secure

Worldwide license and distribution agreement

Celo Communications
Validation authority added to PKI products

Copyright 1999 Thomson Information Services Inc.

COMPANY NAMES: EQUIFAX SECURE INC; INTERNATIONAL BUSINESS MACHINES CORP;
VALICERT INC
INDUSTRY NAMES: Network hardware and software; Software
PRODUCT NAMES: Communications software packages, except networking
(737251); Networking software packages (737255)
CONCEPT TERMS: All company; All intellectual property; Distribution
license; Orders
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/29 (Item 4 from file: 9)

DIALOG(R)File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

02385477 (THIS IS THE FULLTEXT)

Valicert in Pacts with 4 Foreign Certificate Firms
(Valicert (Mountain View, CA) has formed cooperation deals with international information security firms Baltimore Technologies (Ireland and UK), GlobalSign (Belgium), Thawte Certification (South Africa) and Software Agencies Australia)

American Banker, v 164, n 40, p 17

March 02, 1999

DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 615

ABSTRACT:

Valicert Inc (Mountain View, CA) formed cooperation agreements with four international information security companies: Baltimore Technologies (Ireland and UK), GlobalSign (Belgium), Thawte Certification (South Africa) and Software Agencies Australia. The activity shows the quick dissemination of digital certificate technology in foreign markets.

Valicert supports the validation portion of the certificate process. Valicert's deals with the four firms highlight the trend toward greater demand for certificate services outside the US, according to pres/CEO Yosi Amram. Valicert is either establishing or expanding relationships with the four firms, which are selling digital certificate products.

Valicert anticipates its validation business will increase on par with digital certificates. Valicert sells the idea of a validation authority, or VA, which would complement the certificate authority, or CA, whose believability is growing via the efforts of firms like Baltimore, Entrust, and Verisign Inc.

TEXT:

By JEFFREY KUTLER

Valicert Inc. of Mountain View, Calif., announced cooperation agreements Monday with four international information security companies, a sign of the rapid spread of digital certificate technology in foreign markets.

Valicert, which supports the part of the certificate process known as validation, has forged alliances with such U.S.-based vendors as Entegriety Solutions Corp., Entrust Technologies Inc., GTE Internetworking, Intel Corp., and Netscape Communications Corp.

But Valicert and its marketing partners are encountering considerable demand for certificate services elsewhere, particularly in Europe, said Yosi Amram, president and chief executive officer.

Underlining that trend, Valicert is establishing or expanding relationships with four companies that are selling digital certificate products and are based in other countries: Baltimore Technologies of Ireland and the United Kingdom, GlobalSign of Belgium, Thawte Certification of South Africa, and Software Agencies Australia, which is known as SAA.

Mr. Amram said the deals are the fruit of a marketing effort led by Alexander Garcia-Tobar, vice president of international. The two previously worked together at another Silicon Valley venture, Individual Inc. Mr. Garcia-Tobar more recently was the architect of Forrester Research Inc.'s international expansion.

His arrival at Valicert last summer was timely, Mr. Amram said, because Europe's digital certificate and public key infrastructure market "is neck and neck with, if not ahead of, the United States in terms of adoption and development."

"Culturally, the Europeans are more security- and privacy-conscious," he said. "They are further along with smart cards, which creates a good foundation for a certificate-based infrastructure and applications."

And in the Asia-Pacific region, countries such as Australia, Malaysia, and Singapore have launched large-scale public key infrastructure (PKI) and electronic commerce initiatives.

Valicert expects its validation business to grow hand-in-hand with digital certificates, which are data encryption-related credentials for authenticating parties in an electronic transaction. Valicert sells the concept of a validation authority, or VA. It would complement the certificate authority, or CA, which is gaining credence through the efforts of companies like Baltimore, Entrust, and Verisign Inc.

Valicert promotes a technique for ascertaining a certificate's validity—assuring that it is not expired or revoked—called a certificate revocation tree. But the company's products also support OCSP-on-line certificate status protocol—and the certificate revocation list, or CRL, approach.

"Valicert is the recognized leader in digital certificate validation, and

we felt confident in completely outsourcing our global validation requirements to them," said Thawte president and CEO Mark Shuttleworth. With the Valicert Global VA service, he said, customers will be assured of "complete validation integrity" while Thawte can "differentiate its service and focus on its core business of certification."

Mr. Amram said Thawte, No. 2 to Verisign in issuing certificates under the Internet's popular SSL security protocol, is well advanced in cross-certification among different CAs. That could be a boon to Valicert as well.

GlobalSign, formerly Belsign, is No. 3 in public SSL certificates. It will be a Valicert distributor, use Global VA with a CRL system, and bring Valicert into its GlobalSign Ready interoperability program. GlobalSign CEO Anthony Belpaire said the choice of Valicert "is the first step in ensuring that our customers will have instant access to the best validation products on the market.

SAA will be a Valicert distributor for Australia and New Zealand, which Mr. Garcia-Tobar described as "important emerging markets for PKI."

Valicert contributes to SAA's strategy of providing "leading-edge electronic commerce solutions with a universal, scalable family of products," said SAA managing director Bob White. Baltimore "is licensing and embedding our tool kit and using our VA server as their validation solution," Mr. Amram said. One of the fastest-growing certificate companies, Baltimore was named with GlobalSign as CA subcontractors for a major European Union commerce project coordinated by PricewaterhouseCoopers.

Copyright 1999 Thomson Information Services Inc.

COMPANY NAMES: BALTIMORE TECHNOLOGIES; GLOBALSIGN NV; SOFTWARE AGENCIES AUSTRALIA; THAWTE CERTIFICATION; VALICERT INC
INDUSTRY NAMES: Broadcasting; Business services; Computer; Software; Telecommunications
PRODUCT NAMES: Servers (357105); Broadcast (366396); Development support software packages (737224); Data entry, processing and verification services (737423)
CONCEPT TERMS: All company; All intellectual property; Distribution license; Joint venture
GEOGRAPHIC NAMES: Africa (AFRX); Australia & New Zealand (AUNX); Australia (AUS); Belgium (BEL); European Union (EUCX); Ireland (IRE); North America (NOAX); Pacific Rim (PARX); South Africa (SOA); Sub-Saharan Africa (SUSX); United Kingdom (UNK); United States (USA); Western Europe (WEEEX)

7/9/30 (Item 5 from file: 9)

DIALOG(R) File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

02326030 (THIS IS THE FULLTEXT)

Validation Vendor in Deal with GTE Unit

(Valicert Inc and GTE Cybertrust signed formal alliance for digital validation technology)

American Banker, v 163, n 243, p 10

December 22, 1998

DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 495

TEXT:

By JEFFREY KUTLER

Valicert Inc. has gained an attractive outlet for its digital validation technology by signing a formal alliance agreement with the GTE Cybertrust unit of GTE Internetworking.

As a major source of public key infrastructure systems for Internet commerce security, GTE Cybertrust gives Valicert a valuable credibility boost.

Valicert-which has been working at least informally with GTE, Entrust Technologies Inc., Baltimore Technologies, and others in the data security field-is purveyor of a technique called CRT for ascertaining whether a digital certificate is valid.

CRT, for certificate revocation tree, is touted as more streamlined than the certificate revocation lists, or CRLs, incorporated in conventional models of the digital authentication technology. CRLs are seen as too unwieldy and unreliable for the stressful, high-volume conditions that are expected to develop with mass-market on-line commerce.

For the certificate authority that manages the intricacies of issuing and verifying digital credentials, GTE Cybertrust can add Valicert to its service menu and has rights to resell the two-year-old validation company's Enterprise Server. The system can check revocation status by any standard means including CRL, CRT, and On-line Certificate Status Protocol.

"Digital certificate validation is critical to enterprises implementing open PKI (public key infrastructure) solutions to secure transactions among large numbers of users, including employees, customers, partners, and suppliers," said Joe Vignaly, director of marketing and business development for GTE Cybertrust, Needham Heights, Mass.

As a Valicert reseller, "Cybertrust meets the growing needs of our customers," he said, "by providing a one-stop source for both CA (certificate authority) products and services and certificate validation."

"GTE participated in our field trial before this, but now we have a more formal relationship," said Sathvik Krishnamurthy, vice president of marketing and business development for Valicert in Mountain View, Calif. ~~"GTE is the largest company we have done a distribution agreement with."~~ Another is Entegriety Solutions Corp. of San Jose, Calif.

"Our goal is to make our validation solution ubiquitous, and that requires relationships with CAs and tool kit licensees" such as GTE and Intel Corp., Mr. Krishnamurthy added.

Like others in information security, Mr. Krishnamurthy can sound like an evangelist on the subject of "an expanded definition of trust" for electronic commerce. "Our agreements with CAs like GTE reinforce that notion," he said in an interview.

The CRL processing challenge has daunted system developers. Valicert offers one solution. In November, Entrust Technologies of Texas announced several licensing agreements for its CRL Distribution Points patent, a "scalability" measure that Valicert president Yosi Amram said he could support.

Others have proposed different approaches that would do away with revocation lists altogether. But Mr. Krishnamurthy pointed out that virtually all major CA proposals, including the Global Trust Enterprise that eight multinational banks announced in October, are following de facto standards that have validation components.

"A variety of techniques are on offer," said analyst David Ferris of Ferris Associates, San Francisco. Focusing on "an important part of the PKI puzzle, Valicert is carving itself a useful little niche."

Copyright 1998 Thomson Information Services Inc.

COMPANY NAMES: GTE CYBERTRUST SOLUTIONS INC; VALICERT INC
INDUSTRY NAMES: Information industry; Online services
PRODUCT NAMES: On-line service providers (737500)
CONCEPT TERMS: All intellectual property; Patent license
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/31 (Item 6 from file: 9)

DIALOG(R)File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

02133080 (THIS IS THE FULLTEXT)

To Drum Up Interest, Valicert Is Giving Away Its Tool Kit
(Valicert Inc has introduced a new version of its tool kit for testing
certificate revocation within electronic commerce programs)

American Banker, v CLXIII, n 79, p 13

April 28, 1998

DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 602

ABSTRACT:

Valicert Inc has introduced a new version of its tool kit for testing certificate revocation within electronic commerce programs. The new product will support any validation protocol and accommodate certificate revocation lists (CRLs). The new tool kit also will support the On-Line Certificate Status Protocol (OCSB).

To make the product more widespread, the firm is offering the new product free. The firm hopes the move will lead to sales of higher-end products for implementing certificate validation.

TEXT:

By JEFFREY KUTLER

Hoping to put some added momentum behind its digital certification tool, Valicert Inc. is offering its customers more options at a lower price.

Free, to be exact.

The Palo Alto, Calif., company announced the release last week of version 2.0 of its tool kit, which software developers can use to test for certificate revocation within electronic commerce programs.

Valicert contends that digital certificates, the electronic credentials that can verify buyers' and sellers' identities on the Internet, will reach their potential only if accompanied by a highly effective means of ascertaining that a given certificate has not expired or otherwise been revoked.

By giving away its software -- it can be downloaded from the valicert.com Web site -- Valicert is following a high-tech precept for stimulating market development. That could lead to sales of higher-end products for implementing certificate validation. "Getting the tool kit out develops ubiquity and a PKI," or public key infrastructure, Yosi Amram, the company's president and chief executive officer, said in an interview.

In theory, as on-line commerce and associated certificate volumes expand, system operators would then want to buy the high performance levels of Valicert's server system. Or a company validating certificates across business units might turn to Valicert's service bureau.

While the free distribution may be the main attention-grabber, Valicert may

be making an even more significant gesture by rendering its tool kit "universal." It will support any validation protocol and not just the "certificate revocation tree" that Valicert champions.

photo omitted

The 2.0 tool kit thus will accommodate certificate revocation lists, or CRLs, which Valicert has dismissed as a slow legacy technology that will not stand up to the stresses of high-volume commerce. Valicert will also support OCSB, the On-line Certificate Status Protocol, being developed under the auspices of the Internet Engineering Task Force.

Any application developer, whether working on secure virtual private networks or the MasterCard-Visa SET payment protocol, "can use our tool kit to check the validity of any certificate, regardless of the platform they support," Mr. Areram said.

The openness "reflects our ongoing commitment to meeting developers' needs today and in the future for multiple validation and revocation technologies," the Valicert CEO added.

Mr. Amram said legacy systems will have a "clear migration path" to certificate revocation trees or beyond. He views the more elaborate OCSB as "right for high-value financial transactions" such as wholesale wire transfers, where people will be willing to pay a price, including a delay in response time, for a desired level of assurance.

"We have a system of roads that support Ferraris, Chews, and buggies," he said. "For validation we need the equivalent. For some very high percentage of transactions -- I don't know if it is 92%, 95%, 98%--certificate revocation tree is right."

Mr. Amram said market feedback since Valicert started selling its systems last year was favorable, but there was reluctance to "get on the bandwagon of a proprietary solution. "Now anyone has an easy, free, no-risk tool that is open and universal, supporting any protocol."

"Any tool kit has to embrace whatever method is being embraced by the marketplace for revocation management," said Victor Wheatman, an analyst with the Gartner Group of Stamford, Conn. "Valicert is continuing and extending its strategy of addressing revocation management, and the addition of protocols is appropriate."

The move won praise from the Financial Services Technology Consortium, the cooperative research organization of major U.S. banking companies. FSTC president Adam Backenroth of Chase Manhattan Corp. said it "demonstrates the true interoperability that is crucial for the global adoption of electronic commerce in the banking and financial services industry."

Copyright 1998 Thomson Information Services Inc.

COMPANY NAMES: VALICERT INC
INDUSTRY NAMES: Applications software; Software
PRODUCT NAMES: Development support software packages (737224); Financial software packages (737268)
CONCEPT TERMS: All product and service information; Product introduction
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/32 (Item 7 from file: 9)
DIALOG(R) File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

02041823 (THIS IS THE FULLTEXT)

ValiCert Offers New Solutions for Secure Internet Transactions
(ValiCert has introduced ValiCert Server, ValiCert Toolkit and ValiCert Service that assure the validity of digital certificates)

Information Today, v 15, n 1, p 38

January 1998

DOCUMENT TYPE: Journal ISSN: 8755-6286 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 360

TEXT:

ValiCert, Inc., a new company delivering encryption technology and services for assuring the validity of digital certificates, has introduced a comprehensive suite of offerings for certificate validity management. The company has also announced the support of several key industry partners, including Entegriety Solutions, Entrust Technologies, GTE CyberTrust, and Netscape Communications Corporation.

Founded in February 1996 by some of the world's leading cryptographers, ValiCert says its goal is to develop a broad certificate validation and revocation infrastructure for the Internet. The company's technology and services enable users to determine, in a time-critical manner, the validity of X.509 digital certificates for secure electronic communications and commerce. The president and CEO is Yosi Amram, familiar to many in the information industry as the former CEO of Individual, Inc.

ValiCert introduced three core products centered on certificate validity management: ValiCert Server, ValiCert Toolkit, and the ValiCert Service.

The ValiCert Toolkit is targeted at software developers writing applications that consume certificates. By embedding the toolkit into their applications, vendors enable products to efficiently check certificate validity in Internet or intranet communications. ValiCert also provides a comprehensive developer's guide, fully documented code, and access to on-site consulting services.

The ValiCert Server is targeted at enterprises that deploy certificate systems. It provides all the technology necessary for confirmation issuance in an intranet setting. The ValiCert Server constructs a certificate revocation tree from a certificate revocation list and, when requested by client application programs, constructs and issues confirmation of digital certificate status. The ValiCert Server will also be embedded in certificate issuance and management systems utilized by public certificate authorities (CAs).

The ValiCert Service will be targeted at enterprises that are conducting broad-based Internet communications and commerce. It will be a clearinghouse for checking the validity of digital certificates across organizational boundaries. The service will enable certificate issuers to distribute their certificate revocation lists in a timely, secure manner and to make them easily available to applications and to people around the world with whom they wish to conduct business. It will also enable any application accepting certificates, regardless of its source, to be assured of the certificate's validity.

photo omitted

Source: ValiCert, Inc., Sunnyvale, CA, 408/738-2000;
<http://www.valicert.com>.

Copyright 1998 Information Today, Inc.

COMPANY NAMES: VALICERT INC

INDUSTRY NAMES: Network hardware and software; Software

PRODUCT NAMES: Networking software packages (737255)

CONCEPT TERMS: All product and service information; Product introduction
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/33 (Item 8 from file: 9)

DIALOG(R) File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

01976557 (THIS IS THE FULLTEXT)

**Managing Digital Certificates -- ValiCert unveils product, service suite
(ValiCert Inc unveiled the ValiCert Toolkit, ValiCert Server and ValiCert
Services will give users a way to distinguish between valid and
compromised X.509 digital certificates in real time)**

InternetWeek, p 52

October 27, 1997

DOCUMENT TYPE: Journal ISSN: 0746-8121 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 375

TEXT:

Byline: Rutrell Yasin

By the year 2000, there will be millions of digital certificates in use. With that prediction in mind, users and vendors have begun to wonder how they are going to manage them all.

Getting a jump on the pack of vendors that hope to capture the certificate-management market, start-up ValiCert Inc. last week rolled out a suite of products and services designed to solve the certificate-revocation problem.

The ValiCert Toolkit, ValiCert Server and ValiCert Services will give users a way to distinguish between valid and compromised X.509 digital certificates in real time, according to Joseph "Yossi" Amram, ValiCert president and CEO.

Certificates-encrypted electronic signatures that bind a person's or a company's identity to a message or transaction-are an important component for security in transacting business over the Internet or corporate intranets.

Currently, security systems validate certificates by checking them against electronic lists of "bad numbers," known as certificate-revocation lists (CRLs). To verify a certificate, an administrator must obtain the latest list and then use memory-sapping software to sift through the list and ensure that the certificate in question is not on the list.

As the public key infrastructure grows, the number of certificates will expand beyond current systems, according to Michael Goulde, a senior analyst with the Patricia Seybold Group. "As revocation lists get bigger and bigger, the present system is not going to work," Goulde said.

Anticipating a need for a more efficient way to validate certificates, ValiCert launched a "revocation tree" that delegates the job of list checking, Goulde said. This approach makes it easier to identify bad number information contained in multiple CRLs, he said.

Software developers can use the ValiCert Toolkit to embed certificate-validation capabilities into their user applications, ValiCert said.

ValiCert also launched the ValiCert Server, which builds a certificate revocation tree from a certificate revocation list.

ValiCert Services will act as a clearinghouse for checking the validity of certificates. Any application that uses ValiCert technology will be able to request verification of digital certificates from ValiCert servers, according to ValiCert officials.

The tool kit and server are available now; ValiCert Services will ship in the first quarter of 1998. The tool kit costs \$995. The server costs \$9,995 and supports Windows NT and Sun Solaris systems.

Copyright 1997 CMP Publications, Inc.

COMPANY NAMES: VALICERT INC
INDUSTRY NAMES: Computer; Network hardware and software; Software
PRODUCT NAMES: Servers (357105); Networking software packages (737255)
CONCEPT TERMS: All product and service information; Product introduction
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/34 (Item 9 from file: 9)

DIALOG(R)File 9:Business & Industry(R)
(c) 2002 Resp. DB Svcs. All rts. reserv.

01969420 (THIS IS THE FULLTEXT)

Encryption Start-Up Serves Servers

(New encryption start-up aims to provide a service that verifies validity of digital certificates in realtime and offer toolkits and servers to VARs)

Computer Reseller News, p 24

October 20, 1997

DOCUMENT TYPE: Journal ISSN: 0893-8377 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 268

TEXT:

Byline: Charlotte Dunlap

Sunnyvale, Calif. -- A new encryption start-up, launching today, aims to provide a service that verifies the validity of digital certificates in realtime and offer toolkits and servers to VARs.

Staffed with a "Who's Who" of cryptography, ValiCert Inc., based here, will sell its toolkits to developers of commerce systems for added security. It also has signed deals with vendors, including Netscape Communications Corp., to embed ValiCert's encryption server technology into the vendors' servers. And finally, the company will provide a service to anyone involved in communicating via digital certificates, to immediately determine the validity of X.509 digital certificates.

"The core of our technology is the mathematical and cryptographic data infrastructure, called a certificate revocation tree," said Chini Krishnan, chairman, chief technology officer and founder of the company.

The technology securely transfers updated information regarding digital certificates to every computer on its server. ValiCert's technology is able to differentiate between valid and compromised digital certificates, he said.

Digital certificates are encrypted electronic "signatures" that attach the identification of a person or company to their electronic message or transaction.

Also on the ValiCert team are Paul Kocher, co-founder and chief scientist,

who designed the cryptography for Netscape's current security technology, Secure Sockets Layer; and Marty Hellman, the co-inventor of public key cryptography, known as Diffie-Hellman. The ValiCert Toolkit will be offered to VARs and software developers for an annual licensing fee of \$995.

Vendors, including Netscape will release a plug-in for the technology in future versions of its SuiteSpot servers. ValiCert initially will conduct field trials of its verification service, with broad availability slated for 1998.

Copyright 1997 CMP Publications, Inc.

COMPANY NAMES: VALICERT INC
INDUSTRY NAMES: Applications software; Software
PRODUCT NAMES: Applications software packages NEC (737279)
CONCEPT TERMS: All product and service information; Product introduction
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)

7/9/35 (Item 1 from file: 15)

DIALOG(R) File 15:ABI/Inform(R)

(c) 2002 ProQuest Info&Learning. All rts. reserv.

02042923 55134638

Certifying the certificate holder

Sterlicchi, John

Upside v12n7 PP: 118-122 Jul 2000 ISSN: 1052-0341 JRNL CODE: UPS

DOC TYPE: Periodical; Feature LANGUAGE: English RECORD TYPE: Fulltext

LENGTH: 3 Pages

SPECIAL FEATURE: Photograph

WORD COUNT: 2175

ABSTRACT: With estimates for the future of e-commerce spending already possessing nearly as many zeros as a page of binary code, it is not difficult to understand why ValiCert, a company that hopes to receive a tiny fee on each transaction involving digital certificates, is salivating at the prospect. Whether ValiCert will succeed in leveraging its complex e-transaction security technologies to turn itself into an Internet infrastructure powerhouse is hotly debated. But the relatively small company is keeping some fast company.

TEXT: Firm hopes neutrality will bring e-commerce trust, riches.

With estimates for the future of ecommerce spending already possessing nearly as many zeros as a page of binary code, it's not difficult to understand why ValiCert, a company that hopes to receive a tiny fee on each transaction involving digital certificates, is salivating at the prospect.

Whether ValiCert will succeed in leveraging its complex e-transaction security technologies to turn itself into an Internet infrastructure powerhouse is hotly debated. But the relatively small company is keeping some fast company.

The front man for the company, President and CEO Yosi Amram, had already taken one Internet startup, Individual Inc., public before he was brought in to complement the technocrats who created ValiCert.

Amram likes to talk about Individual, which delivered personalized news and information as a first-wave Internet company. While e-tailers were the second wave, the third wave is about making the Internet a trusted place for global commerce. Not coincidentally, that's what ValiCert's about.

Validation Authority

The company has raised more than \$30 million in funding and, with the takeover of Receipt.com at the end of last year, now has three core technologies that enable it to provide e-transaction security before, during and after the event.

ValiCert's initial development was its Validation Authority technology, which, in a nutshell, validates all aspects of a digital certificate transaction, no matter what certification authority issued the certificate.

Chini Krishnan, who is now chairman and chief technology officer, and wellknown cryptographer Paul Kocher, who is chief scientist, founded the company on the belief that validation in the e-world would replicate the credit card business, where validation is a billion-dollar business.

Kocher is famous in cryptography circles and is credited with designing the Secure Sockets protocol used for securing Internet transactions. At ValiCert, Kocher developed its patented technology, the Certificate Revocation Tree, which, simply put, validates first whether the certificate holders are who they say they are and second whether they have the authority to do what they want to do.

According to Eric Hemmendinger, an Aberdeen Group analyst who specializes in security issues, ValiCert solved the problem in the online world that was addressed in the real world by having a driver's license—it validated the certificate user's identification. A complex problem, as Hemmendinger says of a digital certificate: "There's not even a face to put with it. There's no human-to-human interaction, per se, so you can't look at the individual and decide, 'Do I want to trust this person?'"

ValiCert President and CEO Yosi Amram (left) and Chairman and CTO Ciri Krishnan.

That technology became ValiCert's Validation Authority (VA). Says Amram: "There are two things you need to validate. First is to identify that his [or her] credential is still valid. The second thing is authorization. A potential customer might clear the valid identity test, but he or she might be limited to spending over \$10,000. Or he or she can only buy hardware, but not software, or tables but not chairs."

Us Importance

Developing VA technology has enabled ValiCert to sit down with large financial customers and well-known technology partners. But there is a nagging question about the actual size and importance of validation.

For instance, John Pescatore, research director at the Gartner Group, says ValiCert is lucky to be venture capital funded because its original validation market hasn't happened yet. In reality, the business use of digital certificates and PHI [public key infrastructure] is quite low," he says. "So it was an idea that was a little ahead of its time."

One company that believes that ValiCert has no real future is digital certificate giant and ever-increasing competitor VeriSign. VeriSign is one security-sector company with no intentions of cooperating with its Mountain View, Calif., neighbor.

Perhaps that's not too surprising, as several key ValiCert executives previously worked for VeriSign, including Kocher. Sathvik Krishnamurthy, ValiCert's vice president of marketing and business development, becomes coy at the mention of VeriSign. He's unwilling to reveal the number of ex-VeriSign people who now work for ValiCert.

Anil Pereira, vice president of VeriSign's Internet services group, doesn't believe that there needs to be another link in the validation chain and

instead stresses that there has to be a relationship between the issuance of the certificate and the validation of it.

The time lag between the issuing of the certificate and its appearance on a ValiCert directory is "the flaw to their design," says Pereira.

Speed is of the essence, he says, but "the problem is that ValiCert does not have direct access to VeriSign certificates, nor do they have direct real-time access to some other certificates."

Yet despite that perceived conceptual flaw, Pereira says, VeriSign plans a similar approach and will widen the scope of its validation away from just its own certificates to encompass others, if the market wants that. "We have plans to host directories across a range of certificates," he says. However, he added, customers are not asking for the service yet.

Pereira says VeriSign is also becoming more involved in the digital certificate field via its takeover of Signio, which gives it another way to chip away at ValiCert's raison d'etre.

Krishnamurthy says that with its Certificate Revocation Tree technology, ValiCert can distribute "revocation data worldwide very inexpensively, making it highly available for optimal response times."

He also hit back at VeriSign by saying that if customers wanted to check a revoked certificate, that company had only one data center, in Mountain View, which will cause even more critical time lags. "Imagine a world of millions of transactions all occurring at the same time and worldwide," he says. "All bottlenecked on a single point of failure, and in one locale."

That, though, is the problem that ValiCert says it has solved with its technology and a number of key worldwide partnerships.

Believing in VA

If its time comes, the rewards could be huge, says Krishnamurthy. The fees in the validation arena are based on volume. "We charge a flat fee per transaction. And it ramps up with the volume of transactions," says Krishnamurthy.

The Global 2000 businesses and their partners that ValiCert is targeting are also prepared to pay the price for security. Pescatore says businesses were already doubling and tripling their spending on security before e-commerce had taken a hold.

"In the mainframe pre-Internet world, companies were spending between 1 and 3 percent of their IT budget on security," he says. "In this Internet world and even pre-e-business, we see companies spending 5 to 8 percent of those budgets."

"It is a lucrative market both on the product side and increasingly on the services side."

ValiCert believes the time is coming because it is not only rolling out products and services but building its own infrastructure. It expects to double its 120-strong workforce this year and also hopes to double its 70 customers.

It has built its first highly secure data center and begun offering what it calls a Global VA Service, which gives customers an alternative to building and maintaining their own VA system.

But, as Amram says, in Japan, people "may not trust a service provider in Mountain View, California, that they don't know" And that, too, could be said for most other countries in the world.

So ValiCert has been busy signing up affiliates to offer its VA technology within their regions. Among those affiliates are Japanese telecom giant NTT, Hong Kong Post, French conglomerate Thomson, and consultancy PricewaterhouseCoopers.

Additionally, the company is fleshing out deals with a whole host of security and digital certificate companies, such as RSA Security, Entrust Technologies, Baltimore Technologies and Tumbleweed Software, to incorporate the VA with their respective technologies.

However, Gartner's Pescatore is a little skeptical of such relationships. "In the security industry today, there's this rising crescendo of partnerships that are really nothing more than putting each other's logos on each other's Web sites."

Pescatore's view notwithstanding, at least one partner sees real value in the relationship. At IPlanet, part of the Sun Netscape Alliance is bundling VA with its Certificate Management System. "We can go to our customers with a certificate solution that also has the capability for checking the validity of certificates. It's a great marriage," says Amy Millard, director of product marketing for IPlanet's directory and security products.

Aberdeen's Hemmendinger believes that in the context of validation, ValiCert is unique in its neutrality. "They're a third party, and they view themselves as 'Switzerland.' They'll work with anyone's digital certificates," he said.

One-Stop Shop

Last year, though, ValiCert decided it needed to offer its customers more than just validation.

"The ringing message we heard from our customers, our affiliates and our partners was, 'We want a one-stop shop for the entire process,'" says Krishnamurthy.

ValiCert acquired Receipt.com last December for an undisclosed amount. The deal brought with it two interesting technologies that enable ValiCert to offer security during and after the e-transaction.

With its new product, SecureTransport, ValiCert says it has developed the first standards-based high-performance FTP software for secure data transport. SecureTransport provides secure data transfer over intranets, extranets, and the Internet and is used widely in missioncritical production environments.

The second piece to complete the ValiCert puzzle is the digital receipt technology that verifies that the transaction took place. Both parties receive a copy of the receipt and ValiCert keeps one in case there is a legal dispute down the road.

ValiCert maintains a Swiss analogy with its new products. "We're still credential- and certification authority-neutral, so our receipt infrastructure works with certificates from any issuer," Amram says. "Our secure transport uses any certificate authority to encrypt the information with their certificate. So all of these products are actually very analogous and they are CA-neutral."

With the digital receipt technology, ValiCert is once again rubbing shoulders with some major companies as a founding member of the Digital Receipt Alliance, which was announced in January.

Also in the alliance are America Online, Microsoft, Office Depot, RCS and the Hewlett-Packard division, VeriFone. Their stated goal is to deliver an XML-based standard for delivering receipts over the Internet.

The alliance's infrastructure is being put in place now. "Digital receipts are going to be everywhere. The vision is that everything that you do in the commerce world will have a digital receipt somewhere that's generated for you," Amram says.

According to Krishnamurthy, ValiCert has identified financial services and business-to-business e-commerce as the two "sweet spot" areas where customers can utilize its full range of solutions.

In the financial-services arena, ValiCert is working with Identrus, which is a consortium of eight international banks trying to carve out a role for banks in the world of e-commerce. ValiCert is also a supplier to the individual banks in the consortium, which are ABN AMRO, Bank of America, Bankers Trust, Barclays Bank, Chase Manhattan, Citigroup, Deutsche Bank, and Hypo Vereinsbank.

In B-to-B, ValiCert is working with Dell so it can send digital receipts to its corporate customers as soon as the PC maker has received the order. This will enable Dell's customers to check that digital receipt against the invoice they receive when the machines are shipped.

However, it's not just in the world of buying and selling that ValiCert is finding customers. Insurance giant Aetna uses SecureTransport to send encrypted insurance claim files.

Working Toward Success

Aberdeen's Hemmendinger believes ValiCert has to work fast and hard to convince its potential customers it is now more than simply a validation company. Using a house-building analogy, the analyst highlighted the predicament ValiCert was in. The company has gone from being a specialist house framer to a general contractor, and it needs to let the world know, he says.

If it doesn't, it won't be the riches of an IPO that ValiCert's executives and investors can look forward to; it will be a less prestigious takeover. "If they're able to shift their positioning in this marketplace, they can be a very significant company in the future," Hemmendinger says. "But, if they don't do this very, very rapidly, it's likely that they'll be acquired instead of remaining independent."

As is customary with a privately funded company, ValiCert's executives won't discuss its plans for an IPO. Nor would they talk about current revenues, its profit and loss picture, or its future.

Amram, not surprisingly, is confident that the pieces are now in place to guarantee success. "The reason we've been excited is that we've got a unique brand and position. If you talk to people about validation, they think of ValiCert; if it's about digital receipts, they think Receipt.com. Now they are both part of the same thing. There is a lot of technology behind this. This isn't just a dot-com URL type of business. There's a lot of investment. The positioning, the partnership and the momentum that we have are very significant."

ValiCert Inc.

ValiCert provides secure infrastructure technology for e-transactions.

Founded: 1996

URL www.valicert.com

Number of employees- 145

Total venture capital raised: \$30 million

John Sterlicchi is a regular contributor to UPSIDE and works for San Jose-based editorialservices company, Edittech International.

THIS IS THE FULL-TEXT. Copyright Upside Publishing Company Jul 2000

COMPANY NAMES:

Valicert Inc (NAICS:511210)

GEOGRAPHIC NAMES: United States; US

DESCRIPTORS: Software industry; Corporate profiles; Electronic commerce;

Computer security; Digital certificates

CLASSIFICATION CODES: 8302 (CN=Software and computer services); 5250

(CN=Telecommunications systems & Internet communications); 9110

(CN=Company specific); 9190 (CN=United States); 5140 (CN=Security)

PRINT MEDIA ID: 10989

7/9/36 (Item 1 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

07654079 Supplier Number: 63763178 (THIS IS THE FULLTEXT)

ValiCert Chosen by Oblix for Secure and Scalable e-Network Infrastructures.

PR Newswire, pNA

July 31, 2000

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 705

TEXT:

ValiCert's Validation Authority (VA) Technology Integrated With Oblix NetPoint

For Secure e-Business Solution

MOUNTAIN VIEW, Calif., July 31 /PRNewswire/ --

ValiCert, Inc. (Nasdaq: VLCT), a leading provider of end-to-end secure infrastructure solutions for e-Transactions, today announced that Oblix Inc., a leading developer of e-business infrastructure software, has selected ValiCert's VA (TM) technology to be integrated into Oblix NetPoint. This integration enables Oblix NetPoint access to either ValiCert Global VA Service (SM) or ValiCert Enterprise VA (TM) for digital certificate validation. Oblix NetPoint offers enterprise environments access to a single, unified infrastructure for user identity management and policy enforcement in today's complex e-commerce business environments.

"ValiCert has demonstrated its leadership position in helping companies develop secure and scalable e-businesses," said Nand Mulchandani, vice president of product management at Oblix. "We are excited to work with ValiCert, and look forward to taking advantage of their secure framework to enable centralized user identity management and access control."

"By leveraging ValiCert's industry-leading Validation Authority technology, Oblix can now provide businesses with a highly secure infrastructure, that was not available previously," said Sathvik Krishnamurty, vice president of marketing and business development at ValiCert. "By selecting ValiCert's technology, Oblix will be positioned to help their customers securely manage their e-business transformation."

The ValiCert Global VA Suite supports OSCP certificate validation as well as Certificate Revocation Trees (CRTs), and works in tandem with the Oblix NetPoint to give organizations certified protection for their Internet-based commerce and communications. The OSCP standard was created by the Internet Engineering Task Force (IETF) and enjoys broad industry support as a mechanism for validating certificate status on the Internet. As a member of the IETF, ValiCert was actively involved in co-authoring the specification.

About Oblix Inc.

Oblix Inc. is a leading developer of e-business infrastructure software that securely connects the right people to the right resources on e-business networks. Oblix NetPoint is a web access management solution

that provides integrated identity management and policy enforcement, resulting in security, manageability and scalability for e-business networks. Oblix solutions have been successfully deployed at Global 2000 corporations such as Amdahl, Hitachi Computer Products, Hoffmann-La Roche, Kinko's, Parsons Services Company, Tellabs, TransCanada Pipelines LTD, Volkswagen and Xilinx. Oblix investors include Kleiner Perkins Caufield & Byers, Patricof & Co., Cisco Systems, the Intel 64 Fund, Sumitomo Corporation and Novell, Inc. With offices in North America and Europe, Oblix is headquartered in Cupertino, Calif. and can be reached at 408-861-6800. For additional information please visit www.oblix.com.

About ValiCert

ValiCert is a leading provider of secure e-Transaction infrastructure products and services for conducting business safely over the Internet. ValiCert's validation, security and proof offering provides enterprises and service providers with a certificate- and payment-neutral infrastructure for protecting the phases of the e-Transaction life cycle. ValiCert's products and services are available through its direct sales force, resellers and service providers.

ValiCert has technology and marketing alliances with providers and users of security services and products. The company's customers include Global 2000 organizations in financial services, telecom, healthcare and government sectors. ValiCert is headquartered in Mountain View, California, and is available on the World Wide Web at www.valicert.com

NOTE: ValiCert, Validation Authority, Global VA Service, Enterprise VA, and Validation VA Suite are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

Except for historical information, this press release includes forward-looking statements that involve risks and uncertainties, including, but not limited to, the Company's fundamental position, continued success of certain strategies, significance of specific relationships to future success, as well as risks as detailed from time to time in the Company's Securities and Exchange Commission filings. Such statements are indicated by words or phrases such as "anticipates", "estimates", "projects", "believes", "intends", "expects", and similar words and phrases. Actual results may differ materially from management expectations. The Company's revenues could decline significantly if the market does not continue to accept the Company's products and services or if the Company's technology contains undetected bugs or defects. See the Risk Factors described in ValiCert's final Prospectus dated July 27, 2000 for its initial public offering. ValiCert assumes no obligation to update the forward-looking statements in this press release.

COPYRIGHT 2000 PR Newswire Association, Inc.

COPYRIGHT 2000 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Oblix Inc.; ValiCert Inc.

EVENT NAMES: *380 (Strategic alliances)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SIC CODES: 7372 (Prepackaged software)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/37 (Item 2 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

07559705 Supplier Number: 63318790 (THIS IS THE FULLTEXT)

ValiCert Teams with WISEKey to Include Validation Authority Suite for Its Unique Global High-Security PKI Service.

PR Newswire, pNA

July 12, 2000

Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 874
TEXT:

MOUNTAIN VIEW, Calif., July 12 /PRNewswire/ --

ValiCert, Inc., a leading provider of end-to-end secure infrastructure solutions for e-Transactions, and WISEKey SA, a provider of root certification authority services, today announced that WISEKey has selected ValiCert's Global VA (TM) Suite as its Validation Authority service. In addition, WISEKey will include ValiCert's Global VA (TM) Suite as a component of its WISECert product, enabling ValiCert to provide WISEKey's products and services to its existing and new clients. The agreement underscores the complementary nature of the products and services provided by WISEKey and ValiCert. It also highlights the growing industry support for digital certificate validation as a way of building a more secure and complete public key infrastructure (PKI), and demonstrates the companies' shared commitment to the Online Certificate Status Protocol (OCSP), the industry standard for performing real-time certificate validation on the Internet.

"ValiCert and WISEKey have integrated their best of breed security components to create a complete, more secure infrastructure that organizations can use to protect all their e-business activities," said Yosi Amram, president and CEO for ValiCert. "This agreement will further strengthen the importance of certificate validation in conducting trusted e-commerce."

"Integrating ValiCert's award-winning certificate validation capabilities into WISEKey's services is a clear win for e-commerce business everywhere," said Malcolm Hutchinson, Chief Executive for WISEKey. "This agreement makes certificate management easier for our combined customers and further adds to our ability to provide a global service for Certification Authorities. In this respect, we anticipate that that WISEKey and ValiCert will work together on further developments."

WISEKey's Common Global Root(TM) services, together with ValiCert's Certificate validation, strengthens the security of PKI solutions by ensuring that certificates presented by users and applications are current and valid. In the dynamic world of e-commerce, the status of employees, customers and suppliers can change frequently. If an important supplier removes a purchasing manager's access privileges, it is critical that the ex-manager's digital certificate is no longer recognized with any trading partners. Certificate validation technology allows e-commerce PKIs to dynamically check, set or update authorization levels before allowing access. By integrating the ValiCert VA solution with WISEKey's Common Global Root(TM) service for WISEKey Affiliate Certification Authorities, their customers can be ensured of up-to-the-moment validation data for e-business partners.

It is expected that the combination of WISEKey's and ValiCert's technologies will allow the International Telecommunication Union (ITU), an intergovernmental organization, and the World Trade Center (WTC) Geneva to accelerate the development of the ITU-WTC-WISEKey partnership for electronic commerce. Due to the newly announced system, ValiCert can now offer its global Validation Authority Service to the Certification Authorities to be created in connection with the ITU Electronic Commerce for Developing Countries (EC-DC) Partnership Project. A total of 20 million certificates are expected to be generated between users of WTC and Electronic Commerce Centers to be established under the partnership.

The ValiCert Global VA Suite supports OCSP certificate validation as well as Certificate Revocation Trees (CRTs), and works in tandem with the WISEKey Affiliate Certification Authorities to give organizations certified protection for their Internet-based commerce and communications. The OCSP standard was created by the Internet Engineering Task Force (IETF) and enjoys broad industry support as a mechanism for validating certificate status on the Internet. As a member of the IETF, ValiCert was actively involved in co-authoring the specification.

About WISEKey

WISEKey is a privately owned company based in Geneva, Switzerland

that provides Root Certification Authority services to Certification Authorities worldwide. The trustworthiness of WISEKey's services is based on their carefully orchestrated security practices and procedures used exclusively for the issuance of high-security certificates to Certification Authorities and other entities that form part of the operational services of the globally interoperable PKIs below it. As part of WISEKey's security procedures, the Global Root Private Cryptographic Key used to issue certificates is stored in an off-line high-security facility deep in the Swiss Alps.

With such high-security infrastructure in place, WISEKey has signed a partnership agreement with the International Telecommunications Union (ITU) to promote the deployment of PKIs in 188 countries with the intention of expanding the use of secure electronic communications. In doing so, WISEKey is also providing e-commerce solutions based on the mass usage of certification and PKI enabled applications to secure the Internet for e-business. This approach changes the entire dynamics of how the Internet is used and will propel its transactional-based usage into the 21st century. For further information visit <http://www.wisekey.com>.

About ValiCert

ValiCert is a leading provider of secure e-Transaction infrastructure products and services for conducting business safely over the Internet. ValiCert's validation, security and proof offering provides enterprises and service providers with a certificate- and payment-neutral infrastructure for protecting the phases of the e-Transaction life cycle. ValiCert's products and services are available through its direct sales force, resellers and service providers.

ValiCert has technology and marketing alliances with providers and users of security services and products. The company's customers include Global 2000 organizations in financial services, telecom, healthcare and government sectors. ValiCert is headquartered in Mountain View, California, and is available on the World Wide Web at www.valicert.com.

NOTE: ValiCert and Validation VA Suite are trademarks of ValiCert, Inc. 11 other product and brand names are trademarks or registered trademarks of their respective owners.

COPYRIGHT 2000 PR Newswire Association, Inc.

COPYRIGHT 2000 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *ValiCert Inc.

EVENT NAMES: *380 (Strategic alliances)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SIC CODES: 7372 (Prepackaged software)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/38 (Item 3 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

07451157 Supplier Number: 62664003 (THIS IS THE FULLTEXT)

ValiCert Teams With iPlanet(TM) to Include Validation Authority Suite with Market-Leading E-commerce PKI Offering.

PR Newswire, pNA

June 12, 2000

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 869

TEXT:

MOUNTAIN VIEW, Calif., June 12 /PRNewswire/ --

ValiCert, Inc., a leading provider of end-to-end secure infrastructure solutions for e-Transactions, and iPlanet(TM) E-Commerce Solutions, a Sun-Netscape Alliance, today announced plans to include ValiCert's Certificate VA? Suite with the iPlanet(TM) Certificate

Management System software. The agreement underscores the growing industry support for digital certificate validation as a way of building a more secure and complete public key infrastructure (PKI), and demonstrates the companies' shared commitment to the Online Certificate Status Protocol (OCSP), the industry standard for performing real-time certificate validation on the Internet.

Certificate validation strengthens the security of PKI solutions by ensuring that certificates presented by users and applications are current and valid. In the dynamic world of e-commerce, the status of employees, customers and suppliers can change frequently. If an important supplier removes a purchasing manager's access privileges, for example, it is critical that the ex-buyer's digital certificate is no longer recognized with any trading partners. Certificate validation technology allows e-commerce PKIs to dynamically check, set or update authorization levels before allowing access. By integrating the ValiCert Certificate VA with the iPlanet Certificate Management System, customers can be ensured of up-to-the-moment validation data for e-commerce partners.

"ValiCert and iPlanet E-Commerce Solutions have integrated their best of breed security components to create a complete, more secure infrastructure that organizations can use to protect all their e-business activities," said Sathvik Krishnamurthy, vice president of marketing and business development for ValiCert. "This agreement is an endorsement of the importance of certificate validation and of our Validation Authority technology."

"Integrating ValiCert's award-winning certificate validation capabilities into iPlanet's market-leading Certificate Management System is a clear win for e-commerce business everywhere," said Wes Wasson, vice president infrastructure product marketing at iPlanet E-Commerce Solutions. "This agreement makes certificate management easier for our combined customers and further strengthens our position as one of the industry's leading secure e-commerce vendors."

The ValiCert Certificate VA Suite includes ValiCert's Certificate VA Server, which supports OCSP certificate validation as well as Certificate Revocation Trees (CRTs), and works in tandem with the iPlanet Certificate Management System to give organizations certified protection for their Internet-based commerce and communications. The suite also includes the ValiCert Validator, ValiCert VA Publisher and ValiCert Validator Toolkit, giving organizations a solution for upgrading their e-business applications to quickly check the status of any digital certificate.

The iPlanet Certificate Management System is the leading e-commerce PKI solution with more than 20 million licenses sold. Its scalable, flexible, and high performance architecture has made iPlanet the e-commerce security choice of many of the world's leading banks, manufacturers, insurers, government agencies, healthcare groups, telecommunications, and service companies. The iPlanet Certificate Management System is a core component of iPlanet's integrated e-commerce infrastructure product line, incorporating portal, application, Web, and directory services into a single platform for robust e-commerce deployment.

ValiCert's Certificate VA Suite is easy to install and manage through a centralized browser-based installation and administration interface. Validation capabilities can be extended to end-users and existing applications through a simplified administration mechanism. The Certificate VA supports both Solaris(TM) and Windows NT platforms, and can be upgraded to ValiCert's Enterprise VA solution.

The OCSP standard was created by the Internet Engineering Task Force (IETF) and enjoys broad industry support as a mechanism for validating certificate status on the Internet. As a member of the IETF, ValiCert was actively involved in co-authoring the specification.

About iPlanet E-Commerce Solutions

iPlanet E-Commerce Solutions, a Sun-Netscape Alliance, was established in March 1999 by America Online, Inc. (NYSE: AOL) and Sun Microsystems, Inc. (Nasdaq: SUNW) to provide easy-to-deploy, comprehensive e-commerce solutions for the Net Economy. iPlanet E-Commerce Solutions provides the industry's broadest portfolio of e-commerce infrastructure and application software and services. Its iPlanet Messaging, Directory, Web

and Application Server software all enjoy #1 market share positions. For more information, consult the iPlanet E-Commerce Solutions Web site at www.iplanet.com or call 888-786-8111.

About ValiCert

ValiCert is a leading provider of secure e-Transaction infrastructure products and services for conducting business safely over the Internet. ValiCert's validation, security and proof offering provides enterprises and service providers with a certificate- and payment-neutral infrastructure for protecting the phases of the e-Transaction life cycle. ValiCert's products and services are available through its direct sales force, resellers and service providers.

ValiCert has technology and marketing alliances with providers and users of security services and products. The company's customers include Global 2000 organizations in financial services, telecom, healthcare and government sectors. ValiCert is headquartered in Mountain View, California, and is available on the World Wide Web at www.valicert.com.

NOTE: Sun, Sun Microsystems, the Sun logo, iPlanet and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Netscape and the Netscape N logo are registered trademarks of Netscape Communications Corporation in the U.S. and other countries. Other Netscape logos, product names, and service names are also trademarks of Netscape Communications Corporation, which may be registered in other countries.

ValiCert, ValiCert B2B Express, ValiCert Digital Receipt Solutions, ValiCert Receipt Notary, ValiCert Receipt Vault, ValiCert Receipt Toolkit, ValiCert Receipt Service, Validation Authority and SecureTransport are trademarks of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

COPYRIGHT 2000 PR Newswire Association, Inc.

COPYRIGHT 2000 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *ValiCert Inc.

EVENT NAMES: *610 (Contracts & orders received)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SIC CODES: 7372 (Prepackaged software)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/39 (Item 4 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

07305662 Supplier Number: 61938313 (THIS IS THE FULLTEXT)

BCE Emergis Forms Alliance with Validation Authority Leader ValiCert.

Business Wire, p0438

May 8, 2000

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 750

TEXT:

Business Editors

MONTREAL & MOUNTAIN VIEW, Calif.--(BUSINESS WIRE)--May 8, 2000

Joins ValiCert Affiliate Program to Provide Validation

Authority Services

BCE Emergis (TSE:IFM) announced today that it has signed a strategic alliance with California-based ValiCert, a leading provider of end-to-end secure infrastructure solutions for e-Transactions. Based on the agreement, BCE Emergis has become a member of the ValiCert Affiliate Program and will now be able to provide its customers with validation authority (VA) services, thus further enhancing its already significant security services offering and extending the trust and security in business-to-business (B2B) transactions.

VA services enable customers to identify potentially unsecure parties in an electronic transaction by instantly verifying the validity of digital credentials, including digital certificates issued by any certificate authority (CA), within any application, using any protocol, from anywhere in the world.

BCE Emergis' VA services support multiple PKI protocols, including the Online Certificate Status Checking Protocol, CRL distribution, and certificate revocation trees. Through its partnership with ValiCert, BCE Emergis now offers an online digital certificate validation service that supports multi-vendor security certificates, including those from Entrust, IBM, VeriSign/Thawte and Baltimore/CyberTrust.

"Considering the high growth of e-commerce and the need for strong security services, we are committed to broadening our portfolio, building on our existing PKI Hosting & Management Services offering and integrating new technologies such as certificate validation", said Rene Poirier, Senior Vice President, Development, Marketing and Integration, BCE Emergis.

"Security and trust are the main drivers of e-commerce and BCE Emergis intends to position itself as a premier provider in this field."

"We are excited to welcome industry leader BCE Emergis to our Affiliate Program as they will play a key role in our expansion into the Canadian market," said Sathvik Krishnamurthy, vice-president of marketing and business development for ValiCert. "BCE Emergis is a leading Canadian company - as a result, users can now buy services that are from - and based in - Canada."

BCE Emergis already designs and operates PKI Hosting and Management Services on behalf of client organizations and provides them with the infrastructure needed to become their own CA - with their own certification policies. Customers benefit from BCE Emergis' expertise, fast turn-around time, scalability, cross-certification capabilities and economies of scale while maintaining total control over their security policies. BCE Emergis VA Services represent the next step in providing end-to-end solutions to certificate issuers and users.

BCE Emergis broad portfolio of security solutions also includes the BCE Emergis Electronic Business Network (BEBN), a highly secure business network that allows businesses to conduct worry-free e-commerce over the Internet. BEBN is an end-to-end solution designed to reduce the complexity and cost of creating and managing a secure, proprietary network. It is a virtually private TCP/IP-based solution designed to support business-to-business e-commerce in a highly secure environment.

ValiCert is a leading provider of secure e-Transaction infrastructure solutions for e-commerce and other business-to-business and business-to-consumer applications. ValiCert's validation, transaction and proof products and services are designed to work with any certificate authority and e-payment solution to provide protection before, during and after e-Transactions. ValiCert's innovative All-Sourcing(TM) approach delivers its products and services through enterprise software, through an outsourced ASP service, and through an offering for service providers.

ValiCert was one of the first companies to develop a commercially-available Online Certificate Status Protocol (OCSP) validation service and continues to lead a variety of Internet standards efforts. The company is one of the chief authors of the OCSP and the Simple Certificate Validation Protocol (SCVP), and contributed to the XML Data Type Definition (DTD) for digital receipts as a founding member of the Digital Receipt Alliance. ValiCert is headquartered in Mountain View, California, with offices worldwide, and can be reached on the Internet at www.valicert.com.

BCE Emergis delivers network-centric e-commerce services that significantly improve customer processes through secure B2B exchanges. Combining e-commerce, e-payment and security services, BCE Emergis offers clients in the healthcare, financial services, telecommunications and transportation industries a full suite of core and vertical-specific services that are the essential building blocks and infrastructure required for e-commerce. BCE Emergis is one of the top e-commerce providers in North America and its shares are included in the TSE 100 Composite Index. For more information, please refer to www.emergis.com.

This news release contains certain forward-looking statements that

reflect the current views and/or expectations of BCE Emergis with respect to its performance, business and future events. Such statements are subject to a number of risks, uncertainties and assumptions. Actual results and events may vary significantly.

COPYRIGHT 2000 Business Wire

COPYRIGHT 2000 Gale Group

PUBLISHER NAME: Business Wire

COMPANY NAMES: *BCE Emergis

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SPECIAL FEATURES: COMPANY

7/9/40 (Item 5 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06856476 Supplier Number: 58077664 (THIS IS THE FULLTEXT)

ValiCert Launches First Universal Digital Certificate Validation Service And Secure Data Center.

PR Newswire, p7648

Dec 8, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1735

TEXT:

ValiCert's Commercial-Grade Global VA Service Secures Multi-Billion Dollar E-Business Market

MOUNTAIN VIEW, Calif., Dec. 8 /PRNewswire/ -- Ushering in a new era in the age of Internet business, ValiCert, Inc., the leading provider of digital certificate validation solutions, today launched the ValiCert Global VA Service(SM), the first commercially available Validation Authority (VA) that can quickly and easily check the validity of any digital certificate before an application accepts it. The company also announced the inauguration of its new, secure data center, offering enterprises a 24x7 fault-tolerant alternative to building and maintaining their own VA system.

Like the instant authorizations that merchants obtain to complete credit card transactions, the ValiCert Global VA Service provides the real-time, universal digital certificate authorization essential for conducting secure e-business that, until today had been absent from the Internet. The only solution that gives enterprises the ability to validate digital certificates from virtually all issuers, ValiCert's Service catapults the company into the league of leading trusted third-party security providers.

"Certificate validation is an important component in the implementation of a secure and trusted electronic commerce marketplace," said Steve Ryan, senior vice president, technology, e-Visa. "The Global VA Service helps create the kind of environment that allows all parties in an electronic transaction to verify that other participants are authorized and valid participants."

ValiCert's turnkey Global VA Service simply plugs into an organization's existing public-key infrastructure (PKI) without any additional investment. The service then provides complete, efficient and reliable validation of a digital certificate from any certificate authority (CA) using any validation protocol and with any client or server application.

"In the emerging 'net economy, organizations will be interacting with hundreds or thousands of outside entities through automated e-business applications, and will have to process tens or hundreds of thousands of digital certificates of various types from numerous issuers to establish trust in these transactions," said Yosi Amram, president and CEO of ValiCert. "Without ValiCert's Global VA Service, organizations using so-called secure applications based on digital certificates have no convenient, reliable way to determine whether or not the certificates presented to them by partners, customers, clients or vendors are valid

before accepting them."

"The universal certificate validation provided by ValiCert Global VA Service for the General Services Administration Access Certificates for Electronic Services (ACES) and Department of Defense Interim External Certification Authority (IECA) operations is essential for dealing with a variety of suppliers and other outside agencies using certificates from a multitude of different issuers," said Daniel E. Turissini, technical director for Operational Research Consultants, Inc. "With ValiCert, the verification of these certificates is completely transparent, and allows us to achieve the degree of assurance we require for our applications."

The ValiCert Global VA Service works with any "validation-ready" secure e-mail, virtual private network, secure proxy server, secure extranet, secure forms or other e-business applications, including Netscape Enterprise Server and Communicator, Microsoft Outlook and Explorer and Trend Micro's Interscan Web Manager. When the Global VA Service receives a validation request from an application, it instantly checks the certificate revocation information in its database from the leading certificate issuers, including Baltimore Technologies (Nasdaq: BALT), CyberTrust, a GTE company (NYSE: GTE), GlobalSign, Entegriety Solutions, Entrust Technologies (Nasdaq: ENTU), IBM (NYSE: IBM), Microsoft (Nasdaq: MSFT), Netscape (NYSE: AOL), RSA Security (Nasdaq: RSAS), Thawte Certification and Xcert International.

"Industry Canada is leading the world in using digital certificates and signatures as part of its spectrum auction software, and we are demonstrating our leadership as a model user of electronic commerce applications and technology. The universal validation offered by the ValiCert Global VA Service is an integral part of the high-level security we have established for this purpose," said Earl Hoeg, manager, wireless networks, for Industry Canada. "Certificate validation is an essential ingredient of our auction system, and we can achieve it transparently through the Global VA Service."

Secure Data Center

ValiCert maintains and operates its own secure, mission-critical, fault-tolerant data center 24 hours a day, seven days a week, on which enterprises can rely rather than building and hosting a Validation Authority system themselves. ValiCert's physical, network and operations security countermeasures -- including biometrics, layers of firewalls, redundant hardware and software server networks, state-of-the-art intrusion detection technology and rigorous employee background checks -- ensure that the validity status of certificates is fully protected at all times.

The ValiCert Global VA Service is replicated around the globe, with mirroring sites in Europe and Japan, providing high-performance certificate validation wherever an organization needs it.

A Universal Security Solution

The ValiCert Global VA Service offers a complete, turnkey solution that enables enterprises to elevate the trust in secure, Internet-based communications and e-business between them and their partners without having to invest in additional infrastructure. The Service also provides a highly secure, fast, efficient and inexpensive way for enterprises to handle very large volumes of certificate validation and revocation with little or no perceived performance delay.

Through its growing network of relationships with leading certificate authorities (CAs), ValiCert can ensure the best access to the most current certificate information available from the leading vendors.

The ValiCert Global VA Service provides universal confirmation of validation status for any client or server application using digital certificates on the Internet. Premier developers such as Intel, with its CDSA framework; Netscape; Microsoft; Worldtalk and others are already incorporating ValiCert validation access directly into their applications, providing exceptional ease of use and full validation functionality.

ValiCert is the only company to offer support for all of today's popular validation methods, including Certificate Revocation Lists (CRLs), CRL Distribution Points (CRLDP), Online Certificate Status Protocol (OCSP), and ValiCert's own Certificate Revocation Tree (CRT) technology. ValiCert also offers the ability to check certificate status online or offline.

Digital Certificate Validation and PKI

PKI is quickly becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. Until ValiCert, there was no efficient and economical way to check the validity of digital certificates issued by any CA from around the globe. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-business.

Availability and Pricing

The ValiCert Global VA Service is available now. For pricing information, contact ValiCert at sales@valicert.com, or call 877-VALICERT.

About ValiCert, Inc.

ValiCert is the leading provider of universal validation solutions and trusted third-party validation services that enable secure e-business transactions and communications over the Internet. As the pioneer Validation Authority (VA), ValiCert has accelerated the rapid adoption of digital certificates worldwide by providing a broad, highly scalable family of products and services that allow enterprises to instantly verify the validity of digital certificates from any certificate authority, within any application, under any protocol, from anywhere in the world.

ValiCert's technological leadership has resulted in the creation of the industry's first global validation network as well as the development of critical certificate validation technologies, including Certificate Revocation Trees, OCSP, and the powerful set of application-specific, transaction-oriented functions called Stateful Validation(TM).

ValiCert has technology and marketing alliances with leading worldwide providers and users of security services and products. Its customers include Global 2000 organizations in financial services, telecom, healthcare and government sectors. ValiCert is headquartered in Mountain View, California, and is available on the World Wide Web at <http://www.valicert.com>.

NOTE: ValiCert is a trademark of ValiCert, Inc. ValiCert Global VA Service(SM) is a service mark of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

Leading digital certificate issuers and/or members of ValiCert's Affiliate Network who support the launch of ValiCert's Global VA Service include the following:

"Baltimore Technologies was the first company to work with ValiCert to provide validation authority technology as part of its PKI, enabling customers to obtain a combined certificate issuance, management and validation solution from a single source," said John Fallon, director of technical market development for Baltimore Technologies. "This announcement of ValiCert's Global VA Service demonstrates once again their commitment to providing a complete and reliable digital certificate validation offering to customers."

"In today's global, Web-based economy, organizations need the assurances provided by ValiCert's Global VA Service that their critical interactions on the Internet are as safe as traditional paper-based ones," said Peter Hussey, president of CyberTrust, a GTE company. "CyberTrust and ValiCert complement each other in that we are both dedicated to securing worldwide e-commerce, business-to-business, and financial transactions, thereby facilitating true, on-line trusted business communities."

"Entrust supports ValiCert's efforts to help bring trust to e-business through their universal clearinghouse for ensuring the validity of all digital certificates," said Nigel Johnson, vice-president, partner marketing and business development, Entrust Technologies Inc. "The Global VA Service complements Entrust products and services in offering Entrust customers everywhere transparent certificate validation for all their applications."

"ValiCert clearly understands the importance of universal certificate validation, and has created a global solution we can feel comfortable

relying on," said Paul Santinelli, vice president of technology and applications for GlobalCenter, a Global Crossing company. "No one else has such a complete solution that virtually assures it will work with all applications and all certificates from all CAs."

"While most of the industry has focused on establishing trust based on digital certificates, ValiCert has been working on ways to establish trust in the certificates themselves, and now they are making their technology easily available through their Global VA Service," said Carl Kessler, vice president of development, IBM SecureWay. "ValiCert has created a terrific adjunct to every enterprise PKI, a universal service that can validate all certificates for all applications."

"ValiCert's new Global VA service is a natural complement to the certificate issuance and management capabilities provided by the RSA Keon product family," said Scott Schnell, senior vice president of marketing for RSA Security. "Certificate validation plays an important role in creating trusted transactions and communications in the new online economy."

"The universal certificate validation provided by the ValiCert Global VA Service is a breakthrough in establishing trust for online transactions," said Mark Shuttleworth, president and CEO of Thawte Certification. "As a result, our customers will have access to a dedicated, mission-critical validation authority solution, ensuring them of complete certificate validation integrity."

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SIC CODES: 7372 (Prepackaged software)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/41 (Item 6 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06727683 Supplier Number: 56451835 (THIS IS THE FULLTEXT)

ValiCert Ships Third-Generation Validation Authority Solution.

PR Newswire, p1620

Oct 18, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1612

TEXT:

Enterprise VA Suite Works with All Certificate Issuers, Validation Protocols,

Applications and Directories

MOUNTAIN VIEW, Calif., Oct. 18 /PRNewswire/ -- ValiCert, Inc., the leading provider of digital certificate validation solutions, today released its third-generation Enterprise VA Suite(TM) 3.0, the industry's first and only complete system for establishing trust and interoperability of digital certificates used in e-commerce and communications applications. A major milestone in ValiCert's product evolution, Enterprise VA Suite 3.0 sets a new standard for interoperability, provides all the tools developers need to make any application validation-ready and introduces powerful Stateful Validation(TM), a framework for adding flexible policies that add full e-business transaction support beyond simple certificate validation.

ValiCert today also revealed its Enterprise VA Suite is poised to play a critical role in the U.S. government's Access Certificates for Electronic Services (ACES) program, helping to protect the privacy of individuals and businesses by ensuring that all digital certificates are valid before they are accepted by government agencies. ValiCert is teamed with both approved ACES vendors, Digital Signature Trust Co., an affiliate

of Zions Bancorporation, and Operational Research Consultants, Inc. to provide a common public key infrastructure to give the American public electronic access to privacy-related U.S. government information and services.

"Certificate validation is a critical enabler for conducting all forms of e-commerce, especially the coming explosion in business-to-business transactions, and only ValiCert is offering a complete, proven solution," said Sathvik Krishnamurthy, vice president of marketing and business development for ValiCert. "ValiCert's extensive experience, impressive track record and mature product family make us the most trusted name in the industry today."

"DST is pleased to have ValiCert on our ACES team, which gives us the option to use ValiCert's robust validation solution to meet our ACES customers' needs," said Scott Lowry, president and chief executive officer of DST. "With their third-generation product, ValiCert has shown their ability to provide the robust validation capabilities that may be required by a project of such magnitude as ACES."

"ValiCert's Enterprise VA Suite will be an integral part of the total PKI solution ORC is providing to agencies of the federal government, and we are pleased to have ValiCert on our team," said Daniel E. Turissini, vice president of Operational Research Consultants, Inc. "Because of the multivendor nature of this project, it is crucial to have universal validation services, and ValiCert is the perfect solution."

Turissini added: "ValiCert is also key to ORC's strategy to migrate the Navy Acquisition PKI developed and operated by ORC to the DoD PKI. ValiCert's EVA allows us to validate certificates from both the Navy Acquisition PKI and the DoD PKI providing a seamless migration as we secure sensitive data. ValiCert is crucial to ORC's efforts on behalf of the DOD and the US Government."

ValiCert's Enterprise VA Suite is also being used by Global Crossing's complex Web hosting division, formerly Frontier GlobalCenter; by Identrus, the trust and security company with key members in the world's leading financial institutions; as well as other leading enterprises around the world in the financial services, telecommunications, electronic commerce and government sectors. Enterprise VA Suite allows these organizations to establish their own Validation Authority (VA) and achieve a higher level of trust in all the digital certificates they use -- from within and without the organization -- by validating them on an ongoing basis. By using ValiCert's family of digital certificate validation products, these organizations are automatically assured that their e-mail, Web, EDI and other Internet applications are protected by accepting only bona fide and trusted digital certificates.

"ValiCert's Enterprise VA is playing a role in our proof-of-concept for enabling businesses to surmount the final obstacle to business-to-business Internet commerce: certainty about a trading partner's identity," said Kristin Kupres, chief operating and technical officer of Identrus. "Using our worldwide business-to-business trust network, companies will be able to use the Internet to open new markets, reduce transaction costs and create unassailable records of their transactions."

"ValiCert clearly understands what enterprise performance, reliability and scalability really means, and has created a Validation Authority solution we can feel comfortable relying on," said Matt Parnell, vice president of product management of Global Crossing's Global Center division. "No one else has such a complete solution that virtually assures it will work with all applications and all certificates from all CAs."

"ValiCert's Validation Authority provides a clearing-house function for users of digital certificate-based applications," said Eric Hemmendinger, senior analyst at Aberdeen Group. "Automatically confirming the validity of digital certificates issued by multiple suppliers' certification authorities, ValiCert's VA provides a valuable form of insurance critical for enterprises conducting e-business."

Stateful Validation

ValiCert's Enterprise VA Suite 3.0 pushes the envelope for Validation Authority innovation with the introduction of Stateful Validation(TM), a new concept of application-specific certificate validation that goes beyond

simple verification by initiating additional related validating actions based on predefined rules. Made possible by the Enterprise VA's open, extensible architecture, Stateful Validation enables businesses to create their own custom VA server extensions, via an API, to perform precisely the functions they need at any point in the validation process. Examples of the operations made possible by Stateful Validation include: extensive, highly flexible logging for auditing purposes; on-the-fly credit checks for merchant reliability assessment; and rule-based authorization for access control or approval of issuance authority and signature level in a PO application.

"ValiCert's Stateful Validation is yet another example of our leadership in delivering best-of-breed certificate Validation Authority solutions," added ValiCert's Krishnamurthy. "Stateful Validation opens the door to a new universe of applications where context-sensitive certification validation can extend the value and security of engaging in e-commerce."

Universal Certificate Validation

ValiCert's Enterprise VA Suite 3.0, the first complete, universal certificate validation solution, sets a new standard for interoperability, working equally well with any certificate issuance system, validation protocol, directory service and certificate-based application to provide secure, efficient and scalable validity confirmation. ValiCert's Enterprise VA Suite adds full directory integration, proxying and forwarding of OCSP requests to other VAs, and enterprise VA mirroring for full fault tolerance capabilities.

Enterprise VA Suite 3.0 consists of multiple product components, including:

- ValiCert Enterprise VA(TM) -- the flagship component of ValiCert's universal validation solutions, the Enterprise VA enables organizations

- to host their own certificate revocation data for both internal and external queries.

- The ValiCert Validator Suite(TM) -- standalone and plug-in software

- modules that enable existing digital certificate applications to check

- the revocation status of digital certificates.

- ValiCert Validator Toolkit(TM) -- an easy-to-use, high-performance development toolkit that enables quick and easy integration of digital

- certificate validation into existing and new applications.

- ValiCert VA Publisher(TM) -- distributes revocation information on a

- regular basis from any of today's popular CAs to ValiCert's validation service or server.

All the ValiCert Enterprise VA Suite components can be easily integrated into an organization's PKI to add validation functionality to applications that incorporate digital certificates. Using the Enterprise VA, companies around the world can conduct e-business and communicate with their partners over an extranet with confidence.

The Enterprise VA works seamlessly with all certificate authorities, including those from Baltimore Technologies, CyberTrust, GlobalSign, Entegriety Solutions, Entrust Technologies, Microsoft Corporation, the Sun-Netscape Alliance, Thawte Certification and VeriSign, Inc.

The Enterprise VA also provides validity status responses using any of today's popular validation protocols -- Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), CRL Distribution Points (CRLDP) and ValiCert's unique Certificate Revocation Tree (CRT).

As a direct result of the efforts of the ValiCert Directory Partners Program announced in July, the Enterprise VA can store revocation information in its own LDAP directory, or in LDAP directories from any of the industry leaders, including the Sun-Netscape Alliance, Innosoft, PeerLogic, Chromatix and Control Data, among others.

The new ValiCert Validator Toolkit 3.0 features a high-level API and

support for multiple cryptographic libraries that makes it easier than ever before to make any new or existing off-the-shelf or custom built application validation-ready. In addition, ValiCert's suite of ready-to-plug-in desktop and server Validators enable today's Web, e-mail and other popular applications to be validated quickly and easily.

Robust, SSL-based, centralized administration and logging round out the significant enhancements to the ValiCert Enterprise VA. Offering superior, detailed logging facilities made possible by the extensible architecture, organizations can also add their own extensions to provide virtually unlimited detail and logging capabilities.

Digital Certificate Validation and PKI

PKI is becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. Until ValiCert, there was no efficient and economical way to check the validity of digital certificates issued by any CA from anywhere in the world. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

About ValiCert

ValiCert provides a universal, scalable family of products and services for quickly and economically verifying the validity of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable Validation Authority (VA) solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.ValiCert.com>.

NOTE: ValiCert Enterprise VA Suite, ValiCert Validator Suite, ValiCert Validator Toolkit, and ValiCert VA Publisher are trademarks of ValiCert, Inc. All other product and company names are trademarks or registered trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

SIC CODES: 7372 (Prepackaged software)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/42 (Item 7 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06640561 Supplier Number: 55767467 (THIS IS THE FULLTEXT)

Data Security Firm Adds Validation Function.

Kutler, Jeffrey

American Banker, v164, n178, p14

Sept 16, 1999

ISSN: 0002-7561

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 1103

TEXT:

Certco Inc. has added a powerful validation component to its digital trust technology.

The New York data security company, a spinoff of the former Bankers

Trust Corp., introduced CertValidator, a system that assures the validity of a digital certificate presented in an electronic commerce transaction.

Certificate validation has become a critical issue -- for some, a stumbling-block -- in attempts to complete the construction of Internet commerce infrastructures.

In the digital equivalent of the printed credit card "hot lists" of the 1960s and 1970s, an on-line seller might have to consult an unwieldy certificate revocation list, or CRL, to see if a presented credential expired or was revoked. CRLs are widely considered unworkable for large-volume networks that put a premium on speed. A leading alternative is OCSP -- the on-line certificate status protocol -- on which CertValidator is built.

Vendors of public key encryption and digital certificate technologies have taken steps to accommodate non-CRL options like OCSP. Xcert International Inc. of Walnut Creek, Calif., has explicitly avoided CRLs because it views on-line, real-time status checking as essential. One company specializing in validation methods and related support services, Valicert Inc. of Mountain View, Calif., has raised consciousness about the issue with its own technology, certificate revocation trees, as well as OCSP.

Certco differs from Valicert's Validation Authority offering, said Certco senior vice president Jay Simmons, in that it integrates a secure OCSP data repository with the "responder" function.

Yosi Amram, president of Valicert, said, "I and Valicert welcome the entry of Certco into the validation space."

"This helps to further legitimize the business need" and reinforces "a message that Valicert has been conveying to the market for over two years."

Calling CertValidator "the second leg of a product offering" that began with certificate authority systems, Mr. Simmons said, "We believe it will be necessary to know who issued a certificate and to get a positive response that it has been issued."

Among the key benefits would be nonrepudation. A buyer of goods, for example, would be unable to claim improperly or fraudulently after the fact that the transaction did not occur.

In keeping with open interoperability principles, CertValidator can store and manage certificates, CRLs, and status data from all major certificate authority vendors. The president of one of them, Peter Hussey of GTE Corp.'s Cybertrust unit, said the program fits well with its "secure extranet" offerings. "This powerful technology not only gives our customers a flexible option for accelerating their business-to-business e-commerce activities," Mr. Hussey said, "but it also makes them more secure."

"Real-time validation capability within and across public key infrastructures is critical for businesses that intend to engage in high-value e-business transactions via the Internet," said Diana Kelley, senior security analyst with Hurwitz Group Inc. "OCSP support and multivendor interoperability are features that the market should demand."

Richard Salz, the architect of CertValidator, said the system's foundations in standards such as OCSP and LDAP (lightweight directory access protocol) and certification for meeting high-level Federal Information Processing Standards contribute to the all-important flexibility and scalability requirements sought by customers.

Included on a long list of CertValidator operational features are hardware-based data encryption and key storage, tamper-proofing, audit trails, and two trademarked ideas, Fast-Path Revocation and Fast-Path Suspension. The former occurs much faster than the hours or days that a CRL system might take. With the latter, a hold can be placed on a certificate in a critical situation, then quickly lifted to return it to valid status.

Meridien Research senior analyst Octavio Marenzi said OCSP responders and repositories can meet the instantaneous information needs of trading partners only if they are "highly secure, fully interoperable, and scalable. All (those) characteristics appear to be present" in CertValidator.

Certco president and chief executive officer John Herron said CertValidator is an "industrial-strength implementation of OCSP," resulting

from the company's mix of skills in such areas as cryptography, banking, law, software, and risk management.

"Many of our technical advantages are simple in design yet sophisticated in concept, the product of engineers and others who know a lot more than just technology," Mr. Herron said.

Mr. Simmons said the system is not only designed "as a secure repository for managing certificate life cycles across multiple certificate authorities," but also is well suited for "the Identrus model" -- a certificate infrastructure that requires multiple participating banks to be in sync with validation.

Certco, in fact, was instrumental in the formation last year of Identrus LLC, a multinational business-to-business trust consortium that included among the founders Bankers Trust and its Germany-based acquirer, Deutsche Bank.

Mr. Simmons said he views Identrus as one of the likely sparks to growth in commercial use of public key encryption technologies in the coming year. "Y2K will be behind us, and we see the banks moving very aggressively," he said.

Certco relinquished its shareholder position in Identrus to compete on an even footing for the banks' business. A rival, Baltimore Technologies, was designated root-key supplier for the pilot phase, and Valicert won a role for its validation tools.

Mr. Amram described CertValidator as "effectively an OCSP responder product," whereas his company, Valicert, is already into a "third generation" with a multipronged strategy including a server that supports all protocols and a third-party validation authority service.

"OCSP is a key component of Identrus' risk management strategy," said the consortium's chief operations and technology officer, Kristin Kupres. "It's great to see Certco respond to the need for real-time digital certificate validation by advancing this important standard."

?

MOUNTAIN VIEW, Calif. -- The Validation technology supplier Valicert Inc. said it has obtained \$23 million in a mezzanine round of venture capital financing.

Leading the investment group was Lucent Venture Partners, an arm of Lucent Technologies. Other members included Canadian Imperial Bank of Commerce, Financial Technology Ventures, First Analysis, France Telecom, Gemplus, Korea Technology Banking, Mitsui, and Thomson-CSF Ventures.

This money came on top of \$7 million last year from August Capital, Bessemer Venture Partners, Draper Fisher Jurvetson, Intel, and U.S. Venture Partners, all of which were also in the mezzanine round.

"This round of funding will enable Valicert to greatly extend the availability of its Validation Authority solutions, allowing companies around the world to securely conduct business transactions over the Internet," said Jean-Michel Barbier, president of Thomson-CSF Ventures, the investment unit of the French technology company.

Valicert president and chief executive officer Yosi Amram said he is "excited at the breadth and diversity of our new investor syndicate. We expect their financial, technology, and distribution experience to play a critical role as we continue to add value to our business."

Copyright c 1999 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1999 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *CertCo Inc.

EVENT NAMES: *336 (Product introduction)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software); 7372691 (Data Encryption Software)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/43 (Item 8 from file: 16)
DIALOG(R) File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

06419108 Supplier Number: 54918947 (THIS IS THE FULLTEXT)
On-Line Banking: Valicert Adds Allies to Rule the Validation World.
Kutler, Jeffrey
American Banker, v164, n115, p12
June 17, 1999
ISSN: 0002-7561
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 947
TEXT:

Valicert Inc., which is trying to lock up one of the specialty markets associated with electronic commerce security, continues to lengthen its list of strategic allies.

The three-year-old company announced agreements last week with Equifax Secure Inc. and International Business Machines Corp., which itself is a close ally of Equifax Inc.'s digital security offshoot.

On top of a series of other cooperation and distribution agreements in recent months, the latest alliances solidify Valicert's claim to serving as the premier source of certificate validation technology-systems that can be used to verify that a digital certificate has not expired or been revoked.

Most leading vendors of public key infrastructures for digital certificates-including Entrust Technologies Inc., Verisign Inc., Baltimore Technologies PLC, GTE Corp.'s Cybertrust unit, Celo Communications of Sweden, and Thawte Certification-have some form of system-integration or interoperability agreement with Valicert.

In a business rife with strategic alliances because few if any companies can deliver the complete range of data security components by themselves, Valicert's record of cooperation is as extensive as any.

Equifax Secure, for example, licensed Valicert's Enterprise VA Suite 2.0 and will make it available to customers of its e-commerce security program. The division of Atlanta-based Equifax Inc., a leader in the consumer information and credit reporting industries, will also serve as a reseller of Valicert's VA, or validation authority, system.

IBM made its VaultRegistry certificate-issuance system, which is a key element of Equifax Secure's offering, compatible with Valicert products such as Enterprise VA and the Valicert Global VA Service.

By incorporating the Valicert technology, "IBM is able to support a wider range of e-business applications as it provides enterprises with trust around the globe," said Mark Greene, the computer giant's vice president of security.

"Valicert is a recognized leader in providing complete and efficient validation authority solutions for digital certificates," said Equifax Secure general manager Jeffrey Johnson. "We look forward to expanding the scope of our certificate issuance systems"-customers will have the option of acting as their own validation authorities rather than relying on an outside service.

Valicert aims to resolve one of the thorny complications of digital certificate operations. Validation of certificates in public key encryption infrastructures, or PKIs, can be so difficult or inefficient that some security-technology innovators have proposed alternative approaches that do without validation per se.

But PKI methods are well entrenched and gaining new adherents as ecommerce takes hold. Encryption keys for digital certificates, the credentials that banks or other trusted parties issue to vouch for a customer's on-line identity, are standard equipment in Internet browser software, for example. (Browser leaders Microsoft and Netscape are on Valicert's partner list; Microsoft's Internet Explorer 5 has validation built in.) Certificates are required of banks, merchants, and consumers by SET, the Secure Electronic Transaction protocol for Internet credit card

payments.

PKI proponents like Mr. Greene of IBM acknowledge that it could take years for these technologies to get fully established. But Mr. Greene pointed out in a recent interview that "it is possible to get it to work without exposing users to all the complexity."

As long as there are PKIs, validation will be an issue-and it is one of the areas where ingenuity is being applied to reduce the operational burdens.

Valicert itself has adjusted to market demands. The Mountain View, Calif., company initially came on the scene with a validation method called Certificate Revocation Tree, considered a vast improvement over the cumbersome checking of certificate revocation lists, or CRLs. Valicert president and chief executive officer Yosi Amram likened CRLs to the paper "hot card bulletins" that retailers had to consult in the early days of credit cards.

In assembling its validation capabilities, however, Valicert recognized that its revocation trees would not displace CRLs overnight. Meanwhile, a new technique called OCSP-On-line Certificate Status Protocol-gained ground within the Internet Engineering Task Force's standards-setting program. To offer complete coverage, Valicert therefore supports CRL and OCSP.

"By working with Valicert, IBM has expanded the options its global customers have to implement a comprehensive, security-rich solution for engaging in communications and commerce over the Internet," Mr. Amram said last week. "We expect additional companies to rely on IBM and Valicert technology to expand the availability of global validation and intend to continue to work closely with IBM to ensure that our products interoperate effectively to enable world-class solutions for enabling global ebusiness."

Though Valicert had been cooperating at some level with PKI companies almost since its inception, recent announcements took on deeper significance. In March, Thawte of South Africa and GlobalSign of Belgium, which had been testing the validation systems, embarked on more formal integration and distribution arrangements.

Baltimore, a British-Irish PKI leader that participated in the March announcement with a licensing and distribution pact, announced a more comprehensive technology integration on April 27. Citing Valicert's OCSP support, Baltimore marketing vice president Patrick Holahan said the deal "adds an enhanced level of trust to Baltimore Unicert digital certificates."

Also in April, Entrust Technologies of Plano, Tex., joined in a "validation interoperability" announcement, encompassing both the Entrustchampioned CRL Distribution Points methodology and OCSP.

"Our partnership with Valicert brings additional revocation choices to our PKI customers through either CRLDP or OCSP standard formats," said Entrust CEO John Ryan.

In mid-April, Digital Signature Trust Co., a subsidiary of Zions First National Bank of Salt Lake City, said it would add the Valicert VA to its certificate repository architecture.

The repository is "the central point of trust for our customers," said Digital Signature Trust president Scott Lowry. He said the Valicert technology would "increase interoperability and improve the performance of our repository certificate-validation queries."

Copyright c 1999 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1999 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *Valicert Inc.

EVENT NAMES: *480 (Use of services)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *4811523 (Home Banking Service); 7372461 (Banking, Finance & Investment Software)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 514199 (All Other Information Services); 51121 (Software

Publishers)
SPECIAL FEATURES: COMPANY

7/9/44 (Item 9 from file: 16)
DIALOG(R) File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

06165989 Supplier Number: 53992756 (THIS IS THE FULLTEXT)

Valicert in Pacts with 4 Foreign Certificate Firms.

Kutler, Jeffrey
American Banker, v164, n40, pNA
March 2, 1999
ISSN: 0002-7561
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 618
TEXT:

By JEFFREY KUTLER Valicert Inc. of Mountain View, Calif., announced cooperation agreements Monday with four international information security companies, a sign of the rapid spread of digital certificate technology in foreign markets. Valicert, which supports the part of the certificate process known as validation, has forged alliances with such U.S.-based vendors as Entegriety Solutions Corp., Entrust Technologies Inc., GTE Internetworking, Intel Corp., and Netscape Communications Corp. But Valicert and its marketing partners are encountering considerable demand for certificate services elsewhere, particularly in Europe, said Yosi Amram, president and chief executive officer. Underlining that trend, Valicert is establishing or expanding relationships with four companies that are selling digital certificate products and are based in other countries: Baltimore Technologies of Ireland and the United Kingdom, GlobalSign of Belgium, Thawte Certification of South Africa, and Software Agencies Australia, which is known as SAA. Mr. Amram said the deals are the fruit of a marketing effort led by Alexander Garcia-Tobar, vice president of international. The two previously worked together at another Silicon Valley venture, Individual Inc. Mr. Garcia-Tobar more recently was the architect of Forrester Research Inc.'s international expansion. His arrival at Valicert last summer was timely, Mr. Amram said, because Europe's digital certificate and public key infrastructure market "is neck and neck with, if not ahead of, the United States in terms of adoption and development." "Culturally, the Europeans are more security- and privacy-conscious," he said. "They are further along with smart cards, which creates a good foundation for a certificate-based infrastructure and applications." And in the Asia-Pacific region, countries such as Australia, Malaysia, and Singapore have launched large-scale public key infrastructure (PKI) and electronic commerce initiatives. Valicert expects its validation business to grow hand-in-hand with digital certificates, which are data encryption-related credentials for authenticating parties in an electronic transaction. Valicert sells the concept of a validation authority, or VA. It would complement the certificate authority, or CA, which is gaining credence through the efforts of companies like Baltimore, Entrust, and Verisign Inc. Valicert promotes a technique for ascertaining a certificate's validity- assuring that it is not expired or revoked-called a certificate revocation tree. But the company's products also support OCSP-on-line certificate status protocol-and the certificate revocation list, or CRL, approach. "Valicert is the recognized leader in digital certificate validation, and we felt confident in completely outsourcing our global validation requirements to them," said Thawte president and CEO Mark Shuttleworth. With the Valicert Global VA service, he said, customers will be assured of "complete validation integrity" while Thawte can "differentiate its service and focus on its core business of certification." Mr. Amram said Thawte, No. 2 to Verisign in issuing certificates under the Internet's popular SSL security protocol, is well advanced in cross- certification among different CAs. That could be a boon to Valicert as well. GlobalSign, formerly Belsign, is No. 3 in public SSL

certificates. It will be a Valicert distributor, use Global VA with a CRL system, and bring Valicert into its GlobalSign Ready interoperability program. GlobalSign CEO Anthony Belpaire said the choice of Valicert "is the first step in ensuring that our customers will have instant access to the best validation products on the market. SAA will be a Valicert distributor for Australia and New Zealand, which Mr. Garcia-Tobar described as "important emerging markets for PKI." Valicert contributes to SAA's strategy of providing "leading-edge electronic commerce solutions with a universal, scalable family of products," said SAA managing director Bob White. Baltimore "is licensing and embedding our tool kit and using our VA server as their validation solution," Mr. Amram said. One of the fastest-growing certificate companies, Baltimore was named with GlobalSign as CA subcontractors for a major European Union commerce project coordinated by PricewaterhouseCoopers.

COPYRIGHT 1999 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *Valicert Inc.; Baltimore Technologies; GlobalSign; Thawte Certification; Software Agencies Australia

EVENT NAMES: *480 (Use of services)

GEOGRAPHIC NAMES: *1U9CA (California); 4EUUK (United Kingdom); 4EUBL (Belgium); 6SOUT (South Africa); 8AUST (Australia)

PRODUCT NAMES: *6009000 (Financial Services NEC)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 52599 (Other Financial Vehicles)

SPECIAL FEATURES: LOB; COMPANY

7/9/45 (Item 10 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06164492 Supplier Number: 53987590 (THIS IS THE FULLTEXT)

GlobalSign to Offer ValiCert Services and Products to its Clients in Europe.

PR Newswire, p1236

March 2, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1133

TEXT:

MOUNTAIN VIEW, Calif., and BRUSSELS, Belgium, March 2 /PRNewswire/ -- ValiCert, Inc., a leading provider of software and services that enable trust and interoperability of digital certificate applications, and GlobalSign, Europe's leading trusted network of Certificate Authorities (CAs), today announced that GlobalSign is participating in the field trial of the ValiCert Global VA Services(SM), the first worldwide digital certificate validation service. In addition, ValiCert is now participating in the GlobalSign Ready program to achieve interoperability between the two companies' products. GlobalSign has also agreed to distribute ValiCert products and services to its clients throughout Europe. The agreement between GlobalSign and ValiCert means that enterprises will be able to quickly and easily ensure electronic credentials from anywhere in the world.

The GlobalSign Ready program, announced in January 1999, is designed to strengthen the relationship between GlobalSign and its partners, as well as ensure technical compatibility between validation and CA products. Through this program, GlobalSign ensures that its certificates work with all leading software/hardware products, such as browsers, Web servers and S/MIME clients. In addition, through GlobalSign embedded technology, certificate procedures, such as request and lookup, are streamlined and simplified for the vendor and end-users.

The ValiCert Global VA Service provides validation of digital certificates using live data, aggregating an array of certification

revocation list (CRL) data from ValiCert's CA service partners. GlobalSign will use scalable validation services to assure the validity of their customers' certificates across the Internet and will also feed all live data from their CRLs in to the ValiCert Global Validation Service.

As part of today's announcement, GlobalSign will also distribute ValiCert's validation authority (VA) products to its clients throughout Europe, enabling its customers to pick and choose among the best validation products available. GlobalSign will also help European companies to integrate the ValiCert VA functionality into their X.509-enabled products for maximum compatible and security.

"Today all participating CA's in GlobalSign's network have to perform best practices. Trust requires best practices, especially in the validation of our certificates.," said Anthony Belpaire, CEO of GlobalSign. "Selecting ValiCert as a partner and participating in their global digital certificate program is the first step in ensuring that our customers will have instant access to the best validation products on the market."

"This announcement reinforces our commitment to providing a highly reliable certificate validation solution on a global basis," said Yosi Amram, president and CEO of ValiCert. "GlobalSign is a recognized European CA leader, and we look forward to working with them as the validation and CA marketplace continues to mature."

ValiCert Validation Authority Solutions

ValiCert's family of Validation Authority products deliver a universal certificate solution designed to work with any certificate issuance system to provide secure, efficient and scalable validity confirmation. ValiCert's digital certificate validation solutions consist of multiple product components that can be easily integrated into an organization's public-key infrastructure (PKI) to add validation functionality to applications that incorporate digital certificates.

In addition to the ValiCert Global VA Service, ValiCert provides:

- * The ValiCert Enterprise VA(TM) is the core component of ValiCert's universal validation solutions. It enables organizations to host their own certificate revocation data on-site and to conduct high-performance, interoperable certificate validity confirmation. ValiCert Enterprise VA supports CRL, OCSP, and ValiCert's Certificate Revocation Tree (CRT) validation methods.

- * The ValiCert OCSP VA(TM) is an entry-level digital certificate validation solution that brings certificate checking to a broad range of organizations and applications. ValiCert OCSP VA Suite is based on the Online Certificate Status Protocol (OCSP), a new industry standard for validating certificate status on the Internet, and is the first complete, commercial implementation of the OCSP protocol for certificate validation.

- * The ValiCert Validator Suite(TM) consists of both standalone and plug-in software modules that enable existing digital certificate applications to check the revocation status of digital certificates for popular Web, S/MIME-based e-mail and other desktop and server applications.

- * ValiCert VA Publisher distributes CRLs on a regular basis from any of today's popular certificate authorities (CAs) to ValiCert's validation service or server, allowing companies to easily manage multiple CAs through a single management framework without increased IT overhead.

- * ValiCert Validator Toolkit is an interoperable, high-performance development toolkit that enables developers to add digital certificate validation capabilities to Internet commerce and communications applications.

Digital Certificate Validation and PKI

PKI is becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication.

However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

ValiCert's products received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communication magazine's sixth annual Hot Products issue.

About GlobalSign

Headquartered in Belgium, Brussels, GlobalSign was founded in 1996 by the National Federation of Belgian Chambers of Commerce and Industry and NetVision, one of Belgium's leading providers of commercial enterprise-wide Internet security solutions. In 1997, three Belgian investment companies, GIMV, Bruficom and Technicom, joined GlobalSign as shareholders, followed by KBC Bank and Verzekeringen in 1998. The trusted network of CA's comprises: GlobalSign Austria; GlobalSign Lebanon; GlobalSign Luxembourg; GlobalSign Greece; GlobalSign Italia; NLSign in the Netherlands; BelSign in Belgium; TurSign in Turkey; the British Chambers of Commerce; and the Beirut Chambers of Commerce. GlobalSign's Certificate Authority (CA) products and services are based on industry-standard public key management technology. GlobalSign receives worldwide support of software developers, including Microsoft, Netscape, IBM, Oracle and Sun Microsystems. More information about GlobalSign can be found on their Web site at <http://www.globalsign.net>.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.valicert.com>.

NOTE: ValiCert Enterprise VA, ValiCert OCSP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, and ValiCert Validator Toolkit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *4E (Europe)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/46 (Item 11 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06164489 Supplier Number: 53987586 (THIS IS THE FULLTEXT)

Thawte Certification Selects ValiCert's Global VA Service(SM) to Support One-Stop Validation for Digital Certificates.

PR Newswire, p1237

March 2, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1054

TEXT:

ValiCert Global VA Service to Validate Thawte's Server Certificates for Secure

E-Commerce and Communications

MOUNTAIN VIEW, Calif., and CAPE TOWN, South Africa, March 2 /PRNewswire/ -- ValiCert, Inc., a leading provider of software and services that enable trust and interoperability of digital certificate applications, and Thawte Certification, one of the world's largest Internet Certification Authorities (CA), today announced that Thawte has selected the ValiCert Global VA Service(SM) to provide validation authority services to its customers. By offering ValiCert's Service, Thawte will provide its customers with the reliability and performance required for validating digital certificates used in e-commerce and communications transactions 24 hours a day, seven days a week

"ValiCert is the recognized leader in digital certificate validation, and we felt confident in completely outsourcing our global validation requirements to them," said Mark Shuttleworth, president and CEO of Thawte. "As a result, our customers will receive a dedicated, mission-critical validation authority solution, ensuring them of complete certificate validation integrity, while enabling Thawte to differentiate its service and focus on its core business of certification."

ValiCert's Global VA Service delivers an efficient high-performance approach to handling very large volumes of certificate validation with little or no perceived performance delay. The company's Global VA Service Data Center is the world's largest facility dedicated to validation, offering high availability and access by replicating all information to validation sites around the globe. The Data Center leverages state-of-the-art technology around the clock to accommodate very high volumes of validation queries in a secure environment.

"Our universal, standards-based Global VA Service offers the only complete, outsourced validation solution, and, as a result, meets all of Thawte's validation needs -- from secure e-mail and electronic commerce to financial services transactions," said Yosi Amram, president and CEO of ValiCert. "With the addition of Thawte to our family of Internet CA partners, ValiCert's service is available through two of the three largest public CAs in the world, thus increasing the overall level of trust for global e-commerce and communications."

Thawte will provide the ValiCert Global VA Service through its Chained CA program that is designed to enable CAs to issue e-mail or Secure Sockets Layer (SSL) certificates that are immediately trusted by all products that trust Thawte. It will also support the ValiCert Global VA service by directly publishing revocation lists to the service.

ValiCert Validation Authority Solutions

ValiCert's family of Validation Authority products deliver a universal certificate solution designed to work with any certificate issuance system to provide secure, efficient and scalable validity confirmation. ValiCert's digital certificate validation solutions consist of multiple product components that can be easily integrated into an organization's public-key infrastructure (PKI) to add validation functionality to applications that incorporate digital certificates.

In addition to the ValiCert Global VA Service, ValiCert provides:

- * The ValiCert Enterprise VA(TM) is the core component of ValiCert's universal validation solutions. It enables organizations to host their own certificate revocation data on-site and to conduct high-performance, interoperable certificate validity confirmation. ValiCert Enterprise VA supports CRL, OCSP, and ValiCert's Certificate Revocation Tree (CRT) validation methods.
- * The ValiCert OCSP VA(TM) is an entry-level digital certificate validation solution that brings certificate checking to a broad range of organizations and applications. ValiCert OCSP VA Suite is based on the Online Certificate Status Protocol (OCSP), a new industry standard for validating certificate status on the Internet, and is the first complete, commercial implementation of the OCSP protocol for

certificate
validation.

* The ValiCert Validator Suite(TM) consists of both standalone and plug-in software modules that enable existing digital certificate applications to check the revocation status of digital certificates for popular Web,

S/MIME-based e-mail and other desktop and server applications.

* ValiCert VA Publisher distributes CRLs on a regular basis from any of today's popular certificate authorities (CAs) to ValiCert's validation

service or server, allowing companies to easily manage multiple CAs through a single management framework without increased IT overhead.

* ValiCert Validator Toolkit is an interoperable, high-performance development toolkit that enables developers to add digital certificate validation capabilities to their Internet commerce and communications application

Digital Certificate Validation and PKI

PKI is becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

ValiCert's products received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communication magazine's sixth annual Hot Products issue.

About Thawte Certification

Headquartered in Cape Town, South Africa, Thawte Certification is a global provider of digital certificate products, services and solutions that create security, privacy and authentication in electronic commerce. Thawte offers a range of certificate solutions that encompass Internet security, extranet security, e-mail security, and enterprise PKI requirements. Founded in 1995, Thawte is the second largest Internet Certificate Authority (CA) worldwide, with offices in both the United States and South Africa, as well as representation in more than 22 countries. More information about Thawte can be found on the company's Web site at <http://www.thawte.com>.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.valicert.com>.

NOTE: ValiCert Enterprise VA, ValiCert OCSP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, and ValiCert Validator Toolkit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Valicert Inc.
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372000 (Computer Software)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 51121 (Software Publishers)
SPECIAL FEATURES: LOB; COMPANY

7/9/47 (Item 12 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

06160584 Supplier Number: 53974498 (THIS IS THE FULLTEXT)
**ValiCert and SAA Sign Reseller Agreement to Bring Validation Authority
Solutions to Australia and New Zealand.**

PR Newswire, p0173
March 1, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 949
TEXT:

Partnership to Extend Availability of Digital Certificate Validation
Solutions, Professional E-Commerce Consulting
MOUNTAIN VIEW, Calif. and MELBOURNE, Australia, March 1 /PRNewswire/
-- ValiCert, Inc., a leading provider of software and services that enable
trust and interoperability of digital certificate applications, and
Software Agencies Australia (SAA), a firm specializing in the distribution
and support of electronic commerce solutions, today announced an agreement
that provides for SAA to distribute ValiCert products throughout Australia
and New Zealand. As part of this agreement, SAA will offer its customers
ValiCert's family of Validation Authority products, including the ValiCert
Enterprise VA Suite(TM) and ValiCert OCSP VA Suite(TM).

The ValiCert Enterprise VA(TM) is the core component of ValiCert's
universal validation solutions. It enables organizations to host their own
certificate revocation data on-site and to conduct high-performance,
interoperable certificate validity confirmation. The ValiCert Enterprise VA
supports Certificate Revocation List (CRL), OCSP, and ValiCert's
Certificate Revocation Tree (CRT) validation methods.

The ValiCert OCSP VA Suite is an entry-level digital certificate
validation solution that brings certificate checking to a broad range of
organizations and applications. ValiCert's OCSP VA Suite is based on the
Online Certificate Status Protocol (OCSP), an emerging industry standard
for validating certificate status on the Internet, and is the first
complete, commercial implementation of the OCSP protocol for certificate
validation. The ValiCert OCSP VA Suite includes the Validator OCSP VA
Server(TM), ValiCert Validator Suite(TM), ValiCert VA Publisher(TM), and
ValiCert Validator Toolkit(TM).

"Because of the explosion of the Internet, there is a huge demand for
innovative and leading-edge electronic commerce solutions in Australia and
Southeast Asia," said Bob White, managing director of SAA. "Our
relationship with ValiCert enables us to meet this need by providing our
customers with a universal, scalable family of products that are highly
regarded in the electronic commerce marketplace."

"Australia and New Zealand are important emerging markets for PKI,
and we are pleased to partner with SAA to deliver ValiCert's Validation
Authority solutions in these regions," said Alexander Garcia-Tobar, vice
president, international for ValiCert.

ValiCert Validation Authority Solutions

ValiCert's family of Validation Authority products deliver a
universal certificate solution designed to work with any certificate
issuance system to provide secure, efficient and scalable validity
confirmation. ValiCert's digital certificate validation solutions consist
of multiple product components that can be easily integrated into an
organization's public-key infrastructure (PKI) to add validation

functionality to applications that incorporate digital certificates.

In addition to the ValiCert Enterprise VA Suite and the ValiCert OSCP VA Suite, ValiCert provides:

- * The ValiCert Validator Suite consists of both standalone and plug-in software modules that enable existing digital certificate applications to check the revocation status of digital certificates for popular Web, S/MIME-based e-mail and other desktop and server applications.

- * ValiCert VA Publisher distributes CRLs on a regular basis from any of today's popular certificate authorities (CAs) to ValiCert's validation service or server, allowing companies to easily manage multiple CAs through a single management framework without increased IT overhead.

- * ValiCert Validator Toolkit is an interoperable, high-performance development toolkit that enables developers to add digital certificate validation capabilities to their Internet commerce and communications application

- * The ValiCert Global VA Service(SM) is a turnkey service that enables organizations to outsource their validation needs, is currently undergoing a worldwide field trial involving leading public CAs and enterprises in North America, Asia-Pacific and Europe.

Digital Certificate Validation and PKI

PKI is the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. These credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

ValiCert's products received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communication magazine's sixth annual Hot Products issue.

About Software Agencies Australia

Founded in 1996, Software Agencies Australia is an innovative Australian company specializing in the distribution and support of electronic commerce solutions. Based in Melbourne, Australia, the company provides professional services to organizations in Australia, New Zealand, Papua New Guinea, Singapore, Thailand, Malaysia, Indonesia, Vietnam, Sri Lanka, Hong Kong, Taiwan and the Philippines. In addition to sales and marketing support for resellers, Software Agencies Australia provides electronic commerce implementation and integration, messaging solutions, mail-enabled applications, electronic directory solution deployment, and public key certification deployment and security solutions. More information about Software Agencies Australia can be found on the company's Web site at <http://www.software-aus.com.au>.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.valicert.com>.

NOTE: ValiCert Enterprise VA, ValiCert OSCP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, and ValiCert Validator Toolkit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group
PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *Valicert Inc.
GEOGRAPHIC NAMES: *8AUST (Australia); 8NEWZ (New Zealand)
PRODUCT NAMES: *7372000 (Computer Software); 7372640 (Electronic
Commerce Software)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 51121 (Software Publishers)
SPECIAL FEATURES: LOB; COMPANY

7/9/48 (Item 13 from file: 16)
DIALOG(R) File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

06080946 Supplier Number: 53587467 (THIS IS THE FULLTEXT)
**XETI and ValiCert Partner to Provide Java-based OCSP Solutions For Digital
Certificate Validation.**

PR Newswire, p6203
Jan 19, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 897
TEXT:

JKIX Toolkit to Interoperate With ValiCert's Global Validation Authority
Solutions Using New Online Certificate Status Protocol (OCSP)
RSA DATA SECURITY CONFERENCE, SAN JOSE, Calif., Jan. 19 /PRNewswire/
-- XETI, Inc. (Trans Enterprise Technologies, Inc.), the leading provider
of Java toolkits for public key infrastructure (PKI) solutions, and
ValiCert, Inc., the leading provider of software and services that enable
trust and interoperability of digital certificate applications, today
announced a partnership to ensure interoperability between Java client
applications developed with XETI's JKIX toolkit and ValiCert's ValiCert's
Validation Authority solutions using the latest IETF standard for Online
Certificate Status Protocol (OCSP). As a result of the partnership, XETI
will offer its customers a broad and thoroughly tested validation solution
that allows Java-based PKI applications to support fast verification of
digital signatures using OCSP.

ValiCert's Validation Authority solutions include their newly
introduced entry level ValiCert OCSP VA(TM), the ValiCert Enterprise VA(TM)
and the ValiCert Global VA Service(SM).

XETI's JKIX provides the capability to perform a critical component
of certificate validation: checking the certificate revocation status using
the OCSP protocol to communicate with a standards-based OCSP responder
service such as ValiCert's Global VA Service, or with a Validation
Authority product. Revocation status checking using OCSP enables quick
verification of digital signatures and enhances the level of integrity of
any information exchanged over the Internet.

"A fast and simple method for validating digital certificates is
increasingly important to our customers," said Dr. Jeff Pan, XETI's
president and CEO. "By offering support for OCSP in our JKIX toolkit and
ensuring interoperability with ValiCert's Validation Authority solutions,
we can provide them with a fast way to build standards-based, open PKI
solutions in Java."

"We are very pleased to announce this partnership to provide OCSP
solutions in Java," said Yosi Amram, president and CEO of ValiCert. "OCSP
client support in XETI's toolkit offers ValiCert's enterprise customers the
ability to develop and deploy new Java applications while leveraging their
investment in ValiCert's Validation Authority software and services."

About XETI, Inc.

Founded in 1997 and privately held, XETI, Inc. is dedicated to
enabling application vendors and system integrators to rapidly develop
standards-based, open solutions in Java, leveraging public-key
infrastructure (PKI) for highly secure e-commerce and enterprise
collaboration over the Internet. XETI's JKIX is the first Java toolkit to

implement the new PKIX standard, and the first to have successfully passed RSA's S/MIME interoperability tests. Using JKIX, developers can build Java applications, browser applets, or Web server plug-ins (servlets) for tasks such as S/MIME messaging, user authentication, and online transactions without requiring in-depth PKI expertise.

XETI's headquarters are located at 5150 El Camino Real, A-32, Los Altos, CA 94022. XETI, Inc. can be reached at 650-694-6800 or on the Internet at <http://www.xeti.com>.

ValiCert Validation Authority Solutions

ValiCert's family of Validation Authority products provide universal certificate validation solution designed to work with any certificate issuance system to provide secure, efficient and scalable validity confirmation. ValiCert's digital certificate validation solutions consist of multiple product components that can be easily integrated into an organization's public-key infrastructure (PKI) to add validation functionality to applications that incorporate digital certificates.

-- ValiCert Enterprise VA and ValiCert OCSP VA are core components of ValiCert's universal validation solutions. The Enterprise VA is a multi-protocol solution that enables organizations to host their own certificate revocation data on-site and to conduct high-performance, interoperable certificate validity confirmation. The entry-level OCSP VA can be easily upgraded to the functionality of the Enterprise VA suite.

-- The ValiCert Validator Suite(TM) consists of both standalone and plug-in software modules that enable existing digital certificate application to check the revocation status of digital certificates for popular Web, S/MIME-based e-mail and other Internet-based applications;

-- ValiCert VA Publisher(TM) which distributes Certificate Revocation Lists (CRLs) on a regular basis from any of today's popular certificate authorities (CAs) to ValiCert's validation service or server, allowing companies to easily manage multiple CAs through a single management framework without increased IT overhead.

-- ValiCert Validator Toolkit(TM) is an interoperable, high-performance development tool that enables developers to add digital certificate validation capabilities to their Internet commerce and communications application.

-- ValiCert Global VA Service is a turnkey service that enables organizations to easily outsource their validation needs, is currently undergoing a worldwide field trial involving leading public CAs and enterprises in North America, Asia-Pacific and Europe.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.valicert.com>.

ValiCert and the ValiCert logo are registered trademarks of ValiCert, Inc. Enabling Global Private Trust, Certificate Revocation Tree, Freshness Proof, ValiCert Enterprise VA, ValiCert OCSP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, and ValiCert Validator Toolkit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 51121 (Software Publishers)
SPECIAL FEATURES: LOB; COMPANY

7/9/49 (Item 14 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

06080198 Supplier Number: 53584620 (THIS IS THE FULLTEXT)

ValiCert Introduces Two New Products To Make E-Mail and Web Browsers More Secure.

PR Newswire, p5550

Jan 18, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1064

TEXT:

Validation Authority Solutions Assure Validity of Digital Certificates
RSA DATA SECURITY CONFERENCE, San Jose, Calif., Jan. 18 /PRNewswire/
-- Two new products that make e-mail and Web browsers safer to use for Internet commerce and communications, were unveiled today by ValiCert, the leading provider of software and services that enable trust and interoperability of digital certificate applications. The ValiCert E-Mail Safety Kit(TM) is a complete solution for validating S/MIME digital certificates before they are used. The ValiCert Web Safety Kit(TM) is a comprehensive solution that protects users against digital certificates that are no longer valid when users browse SSL-based Web servers or download mobile code. These new ValiCert products enable organizations to more effectively screen their defense systems against invalid certificates before they cause damage.

"Organizations rely on digital certificates for Internet commerce and transactions every day," said Sathvik Krishnamurthy, vice president of marketing and business development for ValiCert. "These new safety kits are specifically designed for organizations with or without their own PKI who are concerned about the potential threats of their users being victimized by invalid digital certificates."

ValiCert E-Mail Safety Kit

The ValiCert E-Mail Safety Kit works with e-mail clients from Microsoft and others to assure that secure messaging solutions are truly secure. The components include:

-- ValiCert OCSP VA(TM) is a Validation Authority product that hosts worldwide e-mail revocation data locally on the enterprise local area network (LAN);

-- ValiCert E-Mail Validator(TM) that transparently plugs-in to leading e-mail clients to confirm the status of every digital certificate that users need to trust; and

-- ValiCert Address Book Validator(TM) that complements desktop anti-virus software and regularly scans digital certificates within e-mail address books.

ValiCert Web Safety Kit

The ValiCert Web Safety Kit adds an important layer of protection to certificate-based security solutions by ensuring that users do not execute network binaries from developers whose software publishing certificates have been revoked. It protects against invalid signed Java applets and ActiveX code. It also checks server Secure Sockets Layer (SSL) certificates to confirm they have not been revoked prior to establishing a secure connection. The components of this solution include:

-- ValiCert OCSP VA Validation Authority product;

-- ValiCert Browser Validator(TM) that transparently confirms the status of every digital certificate received by a Web browser; and

-- ValiCert Web Server Validator(TM) that automatically confirms the status of certificates received by a Web server in SSL client authentication.

Both the Web Safety Kit and the E-Mail Safety Kit include a one-year

subscription to the ValiCert Global VA Service(SM), which provides a worldwide database of invalid Web server, e-mail and mobile code certificates.

ValiCert Validation Authority Solutions

ValiCert's family of Validation Authority products deliver a universal certificate validation solution designed to work with any certificate issuance system to provide secure, efficient and scalable validity confirmation. ValiCert's solutions consist of multiple product components that can be easily integrated into an organization's public-key infrastructure (PKI) to add validation functionality to applications that incorporate digital certificates. They include:

- ValiCert Enterprise VA(TM) and ValiCert OCSP VA(TM) are core components of ValiCert's universal validation solutions. The Enterprise VA is a multi-protocol solution that enables organizations to host their own certificate revocation data on-site and to conduct high-performance, interoperable certificate validity confirmation. The entry-level OCSP VA can be easily upgraded to the functionality of the Enterprise VA suite.

- The ValiCert Validator Suite(TM) consists of both standalone and plug-in software modules that enable existing digital certificate applications to check the revocation status of digital certificates for popular Web, S/MIME-based e-mail and other Internet-based applications.

- ValiCert VA Publisher(TM) distributes Certificate Revocation Lists (CRLs) on a regular basis from any of today's popular CAs to ValiCert's validation service or server, allowing companies to easily manage multiple certificate authorities (CAs) through a single management framework without increased IT overhead.

- ValiCert Validator Toolkit(TM) is an interoperable, high-performance development toolkit that enables developers to add digital certificate validation capabilities to their Internet commerce and communications applications.

- ValiCert Global VA Service(SM) is a turnkey service that enables organizations to easily outsource their validation needs, is currently undergoing a worldwide field trial involving leading public CAs and enterprises in North America, Asia-Pacific and Europe.

Digital Certificate Validation and PKI

PKI is becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. Until ValiCert, there was no efficient and economical way to check the validity of digital certificates issued by any CA from anywhere in the world. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

ValiCert's products received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communication magazine's sixth annual Hot Products issue.

Pricing and Availability

The ValiCert E-Mail and Web Safety Kits are available now. For pricing information, contact ValiCert at sales@valicert.com, or call 1-877-VALICERT.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the

World Wide Web: <http://www.valicert.com>.

ValiCert and the ValiCert logo are registered trademarks of ValiCert, Inc. Enabling Global space Private Trust, Certificate Revocation Tree, Freshness Proof, ValiCert Enterprise VA, ValiCert OCSP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, ValiCert Validator Toolkit, ValiCert E-Mail Safety Kit and ValiCert Web Safety Kit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/50 (Item 15 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06080196 "Supplier Number: 53584618" (THIS IS THE FULLTEXT)

ValiCert Introduces OCSP VA Suite for Digital Certificate Validation.

PR Newswire, p5547

Jan 18, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1134

TEXT:

New Entry-level Validation Authority Solution Extends Certificate Checking To a Broad Range of Users and Applications

RSA DATA SECURITY CONFERENCE, San Jose, Calif., Jan. 18 /PRNewswire/ -- ValiCert, Inc., the leading provider of software and services that enable trust and interoperability of digital certificate applications, today announced the availability of its ValiCert OCSP VA Suite(TM), a new entry-level digital certificate validation solution that brings certificate checking to a broad range of organizations and applications. ValiCert's new product is based on the Online Certificate Status Protocol (OCSP), a new industry standard for validating certificate status on the Internet. With the OCSP VA Suite, users can integrate digital certificate validation checking into their organization's security system, adding the highest level of protection to their Internet-based commerce and communications.

The OCSP VA Suite includes the OCSP VA(TM) server, and is the first complete, commercial implementation of the OCSP protocol for certificate validation. It provides an affordable and scalable validation solution that allows organizations to disable invalid or revoked digital certificates for specific users or entities. It works in tandem with any certificate authority (CA) server to ensure organizations the highest level of trust in their digital certificates.

"As certificate validation becomes more critical for conducting e-commerce and e-business, we wanted businesses of all types to more easily have the option of validating the certificates in use in their enterprises," said Yosi Amram, president and CEO of ValiCert. "Our new OCSP VA Suite provides an excellent, vendor-neutral solution for certificate validation that can be set up easily and scales well with an organization's needs."

ValiCert also announced today that Ascom Systec AG, a leading Swiss-based system integrator for trust services to major European banks and government institutions, will be offering the OCSP VA Suite as part of its trust solutions.

"We are pleased to be a ValiCert OCSP VA Suite customer," said Dr.

Erich Ruetsche, head of the business unit for Information Security of Ascom Systec AG.

"We are combining ValiCert's Validation Authority solutions with our S/MIME and trust solutions. ValiCert has a unique concept for unifying the heterogeneous world of PKI. This is especially important for large customers where these heterogeneous solutions are the rule, not the exception." ValiCert's OCSP VA Suite is easy to install and manage through a centralized browser-based installation and administration interface. Validation capabilities can be easily extended to end-users and existing applications through a simplified administration mechanism. The OCSP VA supports both UNIX and Windows NT platforms, and can be easily upgraded to ValiCert's Enterprise VA(TM) solution.

The OCSP standard was created by the Internet Engineering Task Force (IETF) and enjoys broad industry support as a mechanism for validating certificate status on the Internet. As a member of the IETF, ValiCert was actively involved in co-authoring the specification. The new ValiCert OCSP VA provides the first full commercial version of this standard for clients and servers.

Availability

The OCSP VA Suite pricing starts at \$995, and includes the ValiCert OCSP VA, ValiCert Validator Suite(TM), ValiCert VA Publisher(TM) and ValiCert Validator Toolkit(TM), along with licenses for 200 users. The OCSP VA Suite can be downloaded from ValiCert's Web site, <http://www.valicert.com>. For more information, contact ValiCert at sales@valicert.com or call 1-877-VALICERT.

ValiCert Validation Authority Solutions

ValiCert's family of Validation Authority products provide universal certificate validation designed to work with any certificate issuance system to provide secure, efficient and scalable validity confirmation. ValiCert's digital certificate validation solutions consist of multiple product components that can be easily integrated into an organization's public-key infrastructure (PKI) to add validation functionality to applications that incorporate digital certificates. In addition to the OCSP VA server, ValiCert's products and services include:

- ValiCert Enterprise VA is the core component of ValiCert's universal validation solutions, the Enterprise VA enables organizations to host their own certificate revocation data on-site and to conduct high-performance, interoperable certificate validity confirmation. It supports Certificate Revocation List (CRL), OCSP, and ValiCert's Certificate Revocations Tree(TM) (CRT) validation methods.

- The ValiCert Validator Suite consists of both standalone and plug-in software modules that enable existing digital certificate applications to check the revocation status of digital certificates for popular Web, S/MIME-based e-mail and other desktop and server applications.

- ValiCert VA Publisher distributes CRLs on a regular basis from any of today's popular CAs to ValiCert's validation service or server, allowing companies to easily manage multiple CAs through a single management framework without increased IT overhead.

- ValiCert Validator Toolkit is an interoperable, high-performance development toolkit that enables developers to add digital certificate validation capabilities to their Internet commerce and communications application

- The ValiCert Global VA Service(SM) is a turnkey service that enables organizations to easily outsource their validation needs, is currently undergoing a worldwide field trial involving leading public CAs and enterprises in North America, Asia-Pacific and Europe.

Digital Certificate Validation and PKI

PKI is becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. Until ValiCert, there was no efficient or economical way to check the validity of digital certificates issued by any CA from anywhere in the world. ValiCert's Validation Authority products and services

complement CAs to empower end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

ValiCert's products received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communication magazine's sixth annual Hot Products issue.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.valicert.com>.

ValiCert and the ValiCert logo are registered trademarks of ValiCert, Inc. Enabling Global Private Trust, Certificate Revocation Tree, Freshness Proof, ValiCert Enterprise VA, ValiCert OCSP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, and ValiCert Validator Toolkit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/51 (Item 16 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c). 2002 The Gale Group.. All rts. reserv.

06072150 Supplier Number: 53549592 (THIS IS THE FULLTEXT)

PKI validation suite arrives.

Nelson, Matthew

InfoWorld, v21, n2, p47(1)

Jan 11, 1999

ISSN: 0199-6649

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 512

TEXT:

ValiCert is now shipping its Enterprise VA Suite to address the nagging question of how to validate certificates for public key infrastructure (PKI) and digital certificate systems.

Security analysts have predicted widespread adoption of PKI and digital certificate systems during the next year.

However, according to analysts, certificate adoption is being hampered by the key problem of ensuring that a certificate that one receives is actually valid at the time it was sent.

"It's a deep dark secret of most places that they aren't validating," said Jonathan Penn, a senior research analyst at Ferris Research, in San Francisco. "This is why we are seeing pretty slow acceptance of, most specifically, secure e-mail."

To address this issue, ValiCert's new Enterprise VA Suite supports commonly used validation schemes and does so automatically, according to company officials.

"Our goal here is to provide a complete set of Validators so that customers that receive certificates -- regardless of where they come from -- [can] ask, 'Should I trust this?' " said Sathvik Krishnamurthy, vice president of marketing and business development at ValiCert. "That is what a Validation Authority is all about."

The suite includes an E-Mail Validator, which plugs in to Secure MIME-based e-mail clients; an Address Book Validator, which regularly scans certificates within an e-mail name and address book to see whether they are valid; and a Browser Validator, which allows end-users within a company to be alerted if a commerce server is using a Secure Sockets Layer certificate that has been revoked.

The Browser Validator also alerts users when mobile code is downloaded that has been signed by a revoked certificate authority.

The automated checking of a digital certificate's validity is essential if security is going to be maintained, according to Ferris' Penn.

"The reason this is necessary is that you can always tell someone every time they get a certificate, 'You need to check that,' but people aren't going to do that. So you need to do that automatically," Penn said. "That's what the Validator suite of applications does."

Most important, according to Penn, if companies are going to be using PKI or digital certificates, they need a validation system that works with all types of certificates.

"If you're looking seriously at PKI, then you need to validate the certificates that are being used by other parties," Penn said. "If you don't do that, then you lose your legal resource. It's sort of like accepting a credit card without doing a check on the card. You need the validation solution, and you need it to be automated, too."

The ValiCert Enterprise VA Suite is available now for the Windows NT and Solaris operating platforms, with pricing starting at \$25,000 for 25,000 users and two certificate authorities.

ValiCert Inc., in Mountain View, Calif., can be reached at www.valicert.com.

Certificate validation

Though many require some sort of user interaction, certificates used in PKI systems can be validated today through a variety of means.

- * Certificate revocation lists (CRLs)
- * Online Certificate Status Protocol
- * CRL distribution points
- * Certificate Revocation Tree

Copyright (c) 1999 InfoWorld Media Group Inc.

COPYRIGHT 1999 InfoWorld Publishing Company

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: InfoWorld Publishing Company

COMPANY NAMES: *Valicert Inc.

EVENT NAMES: *336 (Product introduction)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372613 (Network Security Software)

INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation)

NAICS CODES: 51121 (Software Publishers)

TRADE NAMES: Enterprise Validation Server (Network security software)

SPECIAL FEATURES: COMPANY

7/9/92 (Item 17 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06070537 Supplier Number: 53545373 (THIS IS THE FULLTEXT)

ValiCert Ships Enterprise VA Suite 2.0 for Digital Certificate Validation.

PR Newswire, p1617.

Jan 11, 1999.

Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1214
TEXT:

Company's Validation Authority Solution In Use by Enterprise
Customers in U.S. and Overseas

MOUNTAIN VIEW, Calif., Jan. 11 /PRNewswire/ -- ValiCert, Inc., the leading provider of software and services that enable trust and interoperability of digital certificate applications, today announced the availability of its ValiCert Enterprise VA Suite(TM) 2.0, the only comprehensive, scalable and multi-protocol solution for validating digital certificates used in e-commerce and communications. With ValiCert's Validation Authority products, customers can now integrate certificate validation capabilities into their enterprise Public Key Infrastructure (PKI) solutions, ensuring the highest level of trust in their digital certificates.

ValiCert also announced today that a number of major enterprises in the telecom, financial services, electronics and government sectors are using the company's Validation Authority solutions. Among them is NEC's Information Systems Division, which is incorporating ValiCert's digital certificate software into its Certificate Authority (CA).

"Certificate validation is one of the most critical issues facing IT managers who are incorporating PKI into their organization," said Akiyoshi Yamaguchi, senior manager of NEC's Information Systems Division. "By using ValiCert's comprehensive family of Validation Authority products, NEC believes that enterprise security can be enhanced with an added dimension of trust."

"With the general availability of our comprehensive Enterprise VA solution, organizations now have an undisputed, single source for all their validation needs," said Sathvik Krishnamurthy, vice president of marketing and business development for ValiCert. "Increasingly, they are realizing that it is not sufficient to have certificates issued by a reliable CA; a complete PKI solution requires that the certificates be validated on an ongoing basis. Our software allows organizations to be their own Validation Authority, ensuring a complete PKI solution and a higher level of trust in the digital certificates they use in Internet-based commerce and communications."

Digital certificates are the electronic 'passports' that hold the digital keys to protect information used in communications and business transactions conducted over the Internet or corporate intranets. By using ValiCert's family of digital certificate Validation Authority products, organizations are automatically assured that their Internet-based e-mail, EDI, and other Internet applications are protected by valid and trusted digital certificates.

ValiCert Enterprise VA Suite

ValiCert's Enterprise VA Suite is a comprehensive, universal certificate validation solution designed to work with any certificate issuance system to provide secure, efficient and scalable validity confirmation. The Enterprise VA provides validity status responses from any X.509 certificate using any of today's popular validation mechanisms, including Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), and ValiCert's unique Certificate Revocation Tree (CRT) validation solution. CRT technology enables users to create "pre-validated" certificates and is the fastest, least expensive and most efficient method of validating certificates today.

ValiCert's Enterprise VA Suite consists of multiple product components that can be easily integrated into an organization's PKI to add validation functionality to applications that incorporate digital certificates. These include:

- * ValiCert Enterprise VA(TM) -- the core component of ValiCert's universal validation solutions, the Enterprise VA enables organizations to host their own certificate revocation data for both internal and external queries. ValiCert's Enterprise VA allows organizations to disable any suspicious or bad users' certificates used in any application or issued by any CA. Because ValiCert's products support all popular certificate

revocation protocols, the Enterprise VA works seamlessly with CA software from leading vendors including Baltimore Technologies, Entegriety Solutions, GTE Internetworking, Microsoft Corporation, Netscape Communications and VeriSign, Inc.

* The ValiCert Validator Suite(TM) -- consists of both standalone and plug-in software modules that enable existing digital certificate applications to check the revocation status of digital certificates. The suite includes both server and desktop Validators for popular Web, S/MIME-based e-mail and other Internet-based applications. These include the ValiCert E-Mail Validator(TM) that plugs in to popular S/MIME-based e-mail clients; the ValiCert Address Book Validator(TM) that complements traditional desktop anti-virus software to check the revocation status of e-mail name and address books; the Web Server Validator(TM) that verifies the validity of a client's certificate before the commencement of any web-based transaction; and the Browser Validator, a module that ensures that users do not execute network binaries from developers whose software publishing certificates have been revoked. The Browser Validator also alerts users to revoked SSL-enabled Web servers.

* ValiCert Validator Toolkit(TM) -- an interoperable, high-performance development toolkit that enables quick and easy integration of digital certificate validation into existing and new applications. The Validator Toolkit provides enterprise developers and ISVs with comprehensive off-the-shelf software components for easily building Internet/intranet applications that validate digital certificates using an array of established validation mechanisms, including CRLs, OCSP and CRTs.

* ValiCert VA Publisher(TM) -- the VA Publisher distributes Certificate Revocation Lists (CRLs) on a regular basis from any of today's popular CAs to ValiCert's validation service or server. This allows companies to easily manage multiple CAs through a single management framework without increased IT overhead. The ValiCert VA Publisher currently supports all of the major certificate servers, including those from Microsoft, Netscape, and Entrust.

Digital Certificate Validation and PKI

Public Key Infrastructure is becoming the cornerstone of many organizations' security strategy. Digital certificates are the core components of a PKI solution because they verify the identity of a user or organization involved in an Internet-based transaction or communication. However, these credentials can fall into unauthorized hands, or become revoked if an employee leaves an organization. Until ValiCert, there was no efficient and economical way to check the validity of digital certificates issued by any CA from anywhere in the world. ValiCert's Validation Authority products and services complement CAs to enable end-user Internet applications to transparently and reliably validate certificates, thus enabling trust and authenticity to all users of secure communications and e-commerce.

ValiCert's products received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communication magazine's sixth annual Hot Products issue.

The ValiCert Global VA Service(SM), a turnkey service that enables organizations to easily outsource their validation needs, is currently undergoing a worldwide field trial involving leading public CAs and enterprises in North America, Asia-Pacific and Europe.

Pricing and Availability

The ValiCert Enterprise VA Suite is available now. For pricing information, contact ValiCert at sales@valicert.com, or call 1-877-VALICERT.

About ValiCert

ValiCert is the leading provider of software and services that enable trust and interoperability of digital certificate applications. The company's Validation Authority products and services deliver high-performance and economical validation of digital certificates. ValiCert combines validation technology with applications and professional services to create scalable, interoperable solutions that enable secure

e-commerce and communications over the Internet. The company has technology and marketing alliances with leading worldwide providers of security services and products, including major CAs and application vendors. ValiCert is headquartered in Mountain View, Calif. and is available on the World Wide Web at <http://www.valicert.com>.

ValiCert and the ValiCert logo are registered trademarks of ValiCert, Inc. Enabling Global Private Trust, Certificate Revocation Tree, Freshness Proof, ValiCert Enterprise VA, ValiCert OCSP VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Address Book Validator, ValiCert E-Mail Validator, ValiCert Web Server Validator, ValiCert Browser Validator, and ValiCert Validator Toolkit are trademarks of ValiCert, Inc. ValiCert Global VA Service is a service mark of ValiCert, Inc. All other company and product names are trademarks of their respective owners.

COPYRIGHT 1999 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/53 (Item 18 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

06026767 Supplier Number: 53453366 (THIS IS THE FULLTEXT)

Validation Vendor in Deal with GTE Unit.

Kutler, Jeffrey

American Banker, v163, n243, pNA

Dec 22, 1998

ISSN: 0002-7561

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 508

TEXT:

By JEFFREY KUTLER

Valicert Inc. has gained an attractive outlet for its digital validation technology by signing a formal alliance agreement with the GTE Cybertrust unit of GTE Internetworking.

As a major source of public key infrastructure systems for Internet commerce security, GTE Cybertrust gives Valicert a valuable credibility boost.

Valicert-which has been working at least informally with GTE, Entrust Technologies Inc., Baltimore Technologies, and others in the data security field-is purveyor of a technique called CRT for ascertaining whether a digital certificate is valid.

CRT, for certificate revocation tree, is touted as more streamlined than the certificate revocation lists, or CRLs, incorporated in conventional models of the digital authentication technology. CRLs are seen as too unwieldy and unreliable for the stressful, high-volume conditions that are expected to develop with mass-market on-line commerce.

For the certificate authority that manages the intricacies of issuing and verifying digital credentials, GTE Cybertrust can add Valicert to its service menu and has rights to resell the two-year-old validation company's Enterprise Server. The system can check revocation status by any standard means including CRL, CRT, and On-line Certificate Status Protocol.

"Digital certificate validation is critical to enterprises implementing open PKI (public key infrastructure) solutions to secure transactions among large numbers of users, including employees, customers, partners, and suppliers," said Joe Vignaly, director of marketing and business development for GTE Cybertrust, Needham Heights, Mass.

As a Valicert reseller, "Cybertrust meets the growing needs of our

customers," he said, "by providing a one-stop source for both CA (certificate authority) products and services and certificate validation."

"GTE participated in our field trial before this, but now we have a more formal relationship," said Sathvik Krishnamurthy, vice president of marketing and business development for Valicert in Mountain View, Calif. "GTE is the largest company we have done a distribution agreement with." Another is Entegriety Solutions Corp. of San Jose, Calif.

"Our goal is to make our validation solution ubiquitous, and that requires relationships with CAs and tool kit licensees" such as GTE and Intel Corp., Mr. Krishnamurthy added.

Like others in information security, Mr. Krishnamurthy can sound like an evangelist on the subject of "an expanded definition of trust" for electronic commerce. "Our agreements with CAs like GTE reinforce that notion," he said in an interview.

The CRL processing challenge has daunted system developers. Valicert offers one solution. In November, Entrust Technologies of Texas announced several licensing agreements for its CRL Distribution Points patent, a "scalability" measure that Valicert president Yosi Amram said he could support.

Others have proposed different approaches that would do away with revocation lists altogether. But Mr. Krishnamurthy pointed out that virtually all major CA proposals, including the Global Trust Enterprise that eight multinational banks announced in October, are following de facto standards that have validation components.

"A variety of techniques are on offer," said analyst David Ferris of Ferris Associates, San Francisco. Focusing on "an important part of the PKI puzzle, Valicert is carving itself a useful little niche."

Copyright c 1998 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1998 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *GTE Corp.; GTE CyberTrust Solutions Inc.; Valicert Inc.

EVENT NAMES: *610 (Contracts & orders received)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *4811000 (Telephone Service); 7372000 (Computer Software)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 51331 (Wired Telecommunications Carriers); 51121 (Software Publishers)

TICKER SYMBOLS: GTE

SPECIAL FEATURES: LOB; COMPANY

7/9/54 (Item 19 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

05698102 Supplier Number: 50141052 (THIS IS THE FULLTEXT)

ValiCert Announces Certificate Validation Module(TM) for CDSA; ValiCert Technology to be Included in Intel's CDSA Reference Implementation

PR Newswire, p706HSMM002

July 6, 1998

Language: English Record Type: Fulltext

Article Type: Article

Document Type: Newswire; Trade

Word Count: 942

TEXT:

PALO ALTO, Calif., July 6 /PRNewswire/ -- ValiCert, Inc., the leading supplier of software and services for validating digital certificates, today announced the Certificate Validation Module (TM) for CDSA, a digital certificate validation plug-in for the Common Data Security Architecture (CDSA) framework. ValiCert also announced today that Intel Corporation has agreed to incorporate the Certificate Validation Module into the next

version of the CDSA Reference Implementation that Intel makes available to its CDSA licensees. The module incorporates ValiCert's Universal Toolkit(TM) which allows CDSA licensees to easily add efficient digital certificate validation capabilities into their PKI-based security solutions.

The CDSA platform is supported by a number of leading vendors, including Intel, IBM Corporation, Security Dynamics Technologies, Inc. and RSA Data Security, Inc., and enables developers to design to a common application program interface (API) and create interoperable plug-and-play security products.

"This announcement underscores ValiCert's commitment to standards-based technology and our leadership in open certificate validation solutions," said Yosi Amram, president and CEO of ValiCert, Inc. "By making ValiCert's Certificate Validation Module for CDSA available as a plug-in to its reference implementation, Intel will continue to demonstrate its leadership in accelerating the deployment of certificate-based applications for secure e-commerce and communications."

"The CDSA framework is an open architecture that is designed to enable vendors and customers to build and deploy plug-and-play security solutions," said Michael Glancy, general manager, Platform Security Division, Intel. "We expect ValiCert's Certificate Validation Module to enhance interoperable, secure Internet commerce applications across multiple platforms."

"Digital certificate validation is a critical element of any public-key infrastructure," said Scott Schnell, vice president of marketing for RSA Data Security, Inc. "ValiCert's validation module addresses this issue and will make an excellent addition to solutions such as RSA's Certificate Security Suite which supports CDSA."

"The enhanced trust that comes with digital certificate validation will become essential as enterprises move from PKI pilots into full production environments," said Dave Power, senior vice president of marketing and corporate development for Security Dynamics Technologies, Inc. "With ValiCert's CDSA-based solution, customers of our upcoming SecurSight products can easily validate certificates used in their secure communications and commerce transactions."

Common Data Security Architecture

CDSA provides a comprehensive and coherent set of security services that are vital to electronic commerce and other business applications or services. CDSA defines a horizontal, four-layer architecture: applications, layered services and middleware, Common Security Services Manager (CSSM) infrastructure, and security service provider modules. The CSSM is the central infrastructure component which applications use to access the underlying security services, such as crypto and certificate management. A reference implementation of CDSA 1.2 for Windows 95 and Windows NT 4.0 is currently available for review by the industry. The Open Group recently adopted CDSA 2.0 for the development of secure applications that are interoperable, extensible and offer cross-platform support.

Digital Certificate Validation

Digital certificates are being used increasingly as electronic credentials for identification, for payment, and for other communications or business transactions conducted over the Internet or corporate intranets. As with the credit card industry, which developed a way to electronically validate the millions of credit card numbers issued by any bank in the world, the use of digital certificates requires its own clearinghouse network for certificate confirmation so that individuals and businesses can assure the validity of any certificate.

ValiCert's Award-Winning Solution

A pioneer in the emerging area of digital certificate validation, ValiCert's software and services deliver the only universal, high-performance solution available today for validating digital certificates. ValiCert's products and services enable organizations to securely and rapidly manage the validation of digital certificates, and provide enterprise developers and ISVs with the tools to build applications that incorporate certificates. ValiCert's products and services include:

- The ValiCert Universal Toolkit(TM) -- provides developers with

comprehensive off-the-shelf software components for easily building Internet/intranet applications that validate digital certificates using an array of established validation mechanisms;

-- The ValiCert Enterprise Server(TM) -- works with any certificate issuance system to enable high-performance, interoperable certificate validity confirmation; and

-- The ValiCert Global Service(TM) -- enables enterprises conducting broad-based Internet communications and commerce to check the validity of digital certificates across organizational boundaries. A global field trial of the ValiCert Service involving more than a dozen Certificate Authorities (CAs) and leading electronic vendors is currently under way.

The company's products this year received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communications' sixth annual Hot Products issue.

About ValiCert

ValiCert is the leading provider of solutions for validating digital certificates. ValiCert's software and services deliver a universal, high-performance solution for assuring the integrity of secure communications and electronic commerce transactions over the Internet. The company's products support all current approaches for digital certificate validation, including Certificate Revocation Lists (CRLs), the emerging OCSP standard, plus its own unique Certificate Revocation Tree(TM) (CRT) mechanism. ValiCert has partnerships with leading worldwide providers of security services and products. The company is headquartered in Palo Alto, Calif. and is available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

ValiCert, ValiCert Validation Module, ValiCert Universal Toolkit, ValiCert Enterprise Server, Certificate Revocation Tree and ValiCert Global Service are trademarks of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

SOURCE ValiCert, Inc.

-0-

07/06/98

/CONTACT: Patrick Corman of Patrick Corman Marketing & Communications, 650-326-9648, or patrick@cormancom.com, for ValiCert/

/Web site: <http://www.valicert.com/> CO: ValiCert, Inc.; Intel Corporation ST: California IN: CPR SU: PDT

SA...

-- HSMM002 --

3229 07/06/98 08:03 EDT <http://www.prnewswire.com>

COPYRIGHT 1998 PR Newswire Association, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: PR Newswire Association, Inc.

COMPANY NAMES: *Valicert Inc.

EVENT NAMES: *330 (Product information)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372613 (Network Security Software)

INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: COMPANY

7/9/98 (Item 20 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

05684597 Supplier Number: 53110817 (THIS IS THE FULLTEXT)

The 1998 Products of the Year.(Buyers Guide)

Network, pNA(1)

April 1, 1998

ISSN: 1093-8001
Language: English Record Type: Fulltext
Article Type: Buyers Guide
Document Type: Magazine/Journal; Trade
Word Count: 11823
TEXT:

Your network team has a meeting. Perhaps with users, perhaps with your CEO.

Someone spots an opportunity, or sees a problem. What should you do?

Someone has a great idea-- one that's sure to improve how you do business.

Soon it's time to put that idea into practice. That means resources. A budget. New staff.

Certainly overtime, maybe a consultant or two. And you need products and services, too. The best products and services.

Like the 1998 Network Magazine Products of the Year.

THE BEST IDEAS

Throughout the year, the editors, writers, and technical experts behind

Network Magazine see lots of products. Nearly every networking vendor parades through our offices, hawking and hyping their latest and greatest releases. After we see the requisite demonstrations, we select many of the products for a closer look in our lab, visit customer sites, or examine the technology through the eyes of trusted advisors.

After we've viewed, installed, and maintained a year's worth of products and services, we have a good idea of what's best in each category--or at least we can narrow the field to the closest contenders. (Or we know there isn't a clear winner; see our write-up of Server Operating System, page

48). Then we reread our notes, conduct more research, drink gallons of caffeinated beverages, and pick the winners.

We don't look for products with the lowest price, the loudest bells and whistles, or the biggest vendor marketing budget. We just look for the best of what began shipping before the end of 1997. And that's what you'll find in our 11th annual Product of the Year Awards. So when someone has that bright idea, and you need to find the right product or service, you'll know where to look first.

But what about the consistently best companies, those product or service innovators that demonstrate an ability to hit the jackpot numerous times?

For the first time, Network Magazine is recognizing them with a Hall of

Fame Award. -The Network Magazine Editors

ENTERPRISE PC SERVER

Compaq

ProLiant 7000

PC servers are becoming such commonplace objects that you can even buy them over the Web. But even with their ubiquity, these products are hardly commodities. You don't want just any old box sitting at your site running critical applications and storing crucial information.

To stand out from the competition, vendors must support multiple processors and fault-tolerance features to ensure that customers stay in business--something Compaq knows how to do very well.

Compaq's enterprise-level ProLiant servers currently support up to four

200MHz Pentium Pro processors (with an eventual migration to eight processors), but in the benchmark battles with competing servers, the

ProLiant has nonetheless held their own, racking up SPECmarks and other performance numbers competitive with the six-way, eight-way, and 10-way offerings.

The ProLiant 7000 sports most fault-tolerance features we're coming to expect in this class of server, including redundant power supplies, redundant cooling fans, ECC memory, redundant disk arrays, and support for redundant network adapters.

Added to this list is the product's support for PCI Hot Plug

capability, making ProLiant 5000 one of the first servers to offer this feature. If a board that supports the PCI Hot Plug specification fails, you can remove and replace it without powering-down the server.

Compaq is no stranger to the Enterprise PC Server category; having won it last year with the ProLiant 5000, the company has struck gold again. Compaq, P.O. Box 692000, Houston, TX 77269, (281) 370-0670 or (800) 652-6672, www.compaq.com.

----- ENTERPRISE RISC SERVER

Sun Microsystems

Ultra Enterprise 10000

Hey, buddy: Looking for a big server? A really BIG server, with high performance, high availability, and industrial-strength characteristics?

Check out Sun Microsystem's Ultra Enterprise 10000 (also known as Starfire), big brother of last year's Product of the Year winner

Ultra

Enterprise 6000.

When you move beyond Intel-based machines to true enterprise-level servers, you're talking RISC technology. There are many contenders in that weight class, but when it comes to brute strength, the only way you'll step beyond

Starfire is with a mainframe--a solution that requires drastic changes in the way you manage the technology. Sun's solution is, at its heart, a familiar Unix machine.

Starfire's specifications might be sufficient for the main computer on the

Starship Enterprise, with its 64 250MHz UltraSparc 9 processors and 20 terabytes of available online storage. If you're back on Earth in late 20th century, you might be equally excited about Starfire's high availability features (just about everything is redundant and hot-swappable); such features are based on Sun's Dynamic System Domain architecture, which partitions the server into stable, interconnected parts.

We're not alone in recognizing the Ultra Enterprise 10000's unique position; our sister publication, Unix Review, recently selected it as Server of the Year. So, it appears that Sun's not just a Java company after all.

Sun Microsystems, 2550 Garcia Ave., Mountain View, CA 94043, (650) 960-1300 or (800) 821-4643, www.sun.com.

----- DIRECTORY SERVICES

Novell

Novell Directory Services

Available since Novell's first release of NetWare 4.0, Novell

Directory

Services (NDS) is now a mature, widely available, distributed directory service that has a global, all-encompassing view of the network. Now, when a new person joins the organization, the network administrator needs to create the user's account only; access can be granted to whatever servers and volumes are deemed necessary. Similarly, if a user leaves the organization, administrators need to go to only one place to delete the account, rather than remember all the servers on which the user had accounts.

As more networks come to have both NetWare and Windows NT-based servers, network administrators once more wish for a single directory that can manage their whole network. To answer that need, Novell recently developed

NDS for Windows NT, which allows Windows NT domains to be part of the NDS directory tree. NT domains show up as containers in the NDS directory tree; administrators can give users access to NT servers and directories as easily as they could grant access to NetWare servers and volumes.

Synchronization between the NDS directory and the NT domain controller is bidirectional, so if a new user account is created in an NT domain, that account is incorporated into the NDS directory tree automatically.

With this product, Novell shows that it realizes not everyone is running

NetWare anymore, but it wants to make sure customers have a unified directory--no matter what operating system they're using.

Novell, 1555 N. Technology Wy., Orem, UT 84097, (801) 861-7000, www.novell.com.

----- WORKGROUP SERVER

Compaq

ProLiant 1600

Performance, high availability, scalability, manageability--such requirements have typically been associated with departmental-class servers. But, with the popularity of intranets and other demanding applications on the rise, even workgroup servers are expected to deliver such advanced functionality.

One company that is taking workgroup computing to a new level is Compaq with its ProLiant 1600. While other server vendors have come out with high-performance workgroup systems, the ProLiant 1600 delivers the most advanced features in its class, as well as the best investment protection.

Based on the Intel Pentium II 266MHz processor, the ProLiant 1600 is equipped with dual-processing capabilities, giving you plenty of room to scale performance as your users and applications increase. Additionally, its four removable media bays and six expansion slots, along with its

54.6Gbytes of maximum internal storage capacity, make it easy for you to accommodate future needs.

On the performance front, the ProLiant 1600's standards-based High Performance System Architecture design increases throughput among such key subsystems as memory, I/O, and processors by using dual-memory controllers and dual-peer PCI buses, which transfer data between each CPU and subsystem in parallel. It also provides two Ultra/Wide SCSI-3 controllers, which can support transfer rates up to 80Mbytes/sec.

To meet all your high-availability needs completely, all the server's hard drives are hot-pluggable, and a redundant power supply is optional.

As for server management, Compaq continues to provide the widest array of tools and the widest range of NOS support.

Compaq, P.O. Box 692000, Houston, TX 77269, (281) 414-0484 or (800) 652-6672, www.compaq.com.

----- E-MAIL SERVER

Isocor

N-Plex Enterprise Server 1.3

Until recently, e-mail technology has been packaged in proprietary trappings, causing e-mail products to be hindered by problems when required to communicate outside their own domain. In the past, open-standards-based e-mail did exist, but the POP-3-based products on the market were utilitarian at best and limited at worst.

Today, we are witnessing an evolution in e-mail technology. The rise of the

Internet as the network of networks and the development of feature-rich

Internet e-mail protocols, such as Internet Message Access Protocol (IMAP-4), has led to a new breed of e-mail products that offer the amenities of proprietary products, while being rooted in Internet technology.

No product illustrates this as well as Isocor's N-Plex. Isocor's package offers a full-strength Internet e-mail package that's ready for the enterprise. N-Plex provides both an SMTP and X.400 messaging system, as well as IMAP-4 and POP-3 message stores, which allow you to choose from a host of e-mail clients, browsers, and applications to access e-mail. In addition, it also includes a Lightweight Directory Access Protocol

(LDAP)-compliant directory service or an optional X.500-based Global Directory Services.

The real strength of the product lies in its Isocor management program, which provides centralized management of multiple, remote N-Plex

e-mail servers. Using this program, network managers can install and configure e-mail servers across the enterprise from a single location. And, the program allows for remote monitoring and management.

Isocor, 3420 Ocean Park Blvd., Santa Monica, CA 90405, (310)
581-8100, www.isocor.com.

----- GROUPWARE

Lotus Development
Domino 4.6

For many people, Lotus is synonymous with groupware. For years, Lotus Notes set the standard for collaborative software, and now Domino has earned it that mantle. Lotus Domino 4.6 offers the same database access, workflow, messaging, and calendaring features that made Notes a winner; it also provides Web capabilities, new administration features, and enhanced development tools.

Domino supports a variety of clients and devices, including Web browsers,

Notes clients, POP-3 and Internet Message Access Protocol 4 (IMAP-4) mail clients, and it now offers a Web site creation tool and a faster HTTP server. Additionally, Lotus has improved security by supporting Secure Sockets Layer (SSL) 3.0 and X.509 certificates.

Domino also has improved administration capabilities. It now features a simplified, step-by-step configuration process, and it uses a single directory to manage all resource directory information for server and network configuration, application management, and security. It includes user account synchronization between Windows NT and Domino, and it is Lightweight Directory Access Protocol (LDAP)-compliant.

In addition to its nifty client and administration features, Domino 4.6 runs on all major platforms and offers outstanding development tools. Lotus has improved Domino's application templates and offers two new optional tools: Lotus BeanMachine for Java, which lets developers create multimedia

Java applets without writing any Java code, and Notes Global Designer, which allows applications to run in different languages synchronously.

By integrating Web capabilities with Domino's already strong proprietary features and development tools, Lotus has once again set the standard for groupware.

Lotus Development, 55 Cambridge Pkwy., Cambridge, MA 02142, (617)
577-8500, www.lotus.com.

----- UNIFIED MESSAGING

Applied Voice Technology
CallXPress for Windows NT

Since telephony is the trickiest element to get right with unified messaging, it makes sense that long-time voice mail vendor Applied Voice

Technology (AVT) is at the forefront of the move to bring together e-mail, fax, and voice into one comprehensive messaging system. By combining its voice expertise with the RightFax network fax product and Windows interface and NT operating system, AVT has come up with a powerful and scalable product.

CallXPress for Windows NT allows a user to access all three message types from either a PC or telephone. When using a PC, the Desktop Message Manager feature allows the user to record and play back voice messages, sort messages by category, create custom message folders, control the speed and volume settings during playback, and archive messages for storage. And, when using a telephone, one can listen to e-mail messages, reply to e-mail with voice messages, and forward fax messages to a fax machine.

By incorporating RightFax (which AVT acquired in 1996) into the mix, CallXPress for Windows NT also offers some impressive fax features, such as allowing users to view faxes confidentially on their PCs and manage faxes from e-mail or any Web browser.

CallXPress for Windows NT runs on NT 4.0 or higher and supports up to 64 ports. It provides a GUI for system management, and multiple CallXPress systems can be administered remotely from a single access point.

Applied Voice Technology, 11410 N.E. 122nd Wy., Kirkland, WA 98034,
(425) 820-6000, www.appliedvoice.com.

----- MANAGEMENT PLATFORM
Computer Associates
CA-Unicenter TNG

In the last two years, Computer Associates (CA) has outflanked its competitors in the systems and network management arenas by coming out with a family of offerings that provides highly integrated control over the combination of end nodes (where systems management once reigned) and interconnecting fabric (the traditional bailiwick of network management).

Enterprise customers who want to configure, monitor, and troubleshoot their business processes got fed up with the finger-pointing that seems to be inherent in having two distinct management regimes.

In the summer of 1997, CA began giving away copies of the Unicenter TNG

Framework, a surprisingly complete set of management tools that forms the foundation for the full (chargeable) Unicenter TNG, as well as for add-on products from CA and third-party developers. The Framework includes auto-discovery of IP and IPX nodes; the 2D and 3D Real World Interface, which has the capability to define business process views; the alert and message dispatch system; the object-based repository; browsers that retrieve information from desktop systems using SNMP or Desktop Management

Interface (DMI) 2.0; a scheduling module that can define policies and kick off events; and a report generator. The strategy is to provide a widely installed management foundation for which third parties can develop products--not unlike the way Windows and Windows NT proliferated.

Unicenter TNG is a comprehensive management solution, but if you find that particular CA module less suitable to your needs than another one, chances are CA has an alliance with the other provider--which means the module can plug into Unicenter with little disruption.

Computer Associates, One Computer Associates Plaza, Islandia, NY 11788,
(516) 342-5224, www.cai.com.

----- SYSTEMS MANAGEMENT
Hewlett-Packard
OpenView ManageX

The idea behind Windows NT servers is that they make it easy for an organization to drop in any number of special-purpose servers--Web servers, mail servers, database servers, and so forth--wherever they may be needed.

Unfortunately, NT Server's native administration tools are designed to work with only one server at a time, which can make it quite tiresome to move from server to server to monitor or troubleshoot. OpenView ManageX takes advantage of NT's Microsoft Management Console (MMC) interface and

Microsoft's Distributed COM (DCOM), enabling network managers to monitor various elements of servers and applications, define alarms for particular events, and set policies that respond to events.

Microsoft's model for MMCs is one-to-one; each server requires one console.

The ManageX console is one-to-many, easing remote administration as well as combining views of servers for more efficient management. The Smart Broker component of ManageX enables administrators to install various "snap-in" modules, including performance logging, rebooting, correlated event logging, confirmed message routing, and application policy monitoring.

Because Windows NT and future versions of Windows 95 have native DCOM functionality, this kind of management information, readily available in a single node, can be carried across the network in its full richness without an SNMP or DMI infrastructure.

HP has made some aggressive acquisitions in the desktop and server systems management field in recent months, including this product from NuView.

OpenView ManageX is a new and highly promising approach to

effectively administering Windows desktops, servers, and applications.
Hewlett-Packard, 300 Hanover Street, Palo Alto, CA 94304, (650)
851-1501 or
(800) 637-7740, www.hp.com/go/openview.

----- ASSET/DESKTOP MANAGEMENT

Intel

LANDesk Management Suite 6.0

For both financial and administrative reasons, desktop asset management is a critical task. Every workstation and server in your organization is a corporate asset, representing capital investment in hardware and software.

In addition, each computer represents a certain amount of workload in terms of maintenance and management. The majority of desktop asset management products are software suites assembled from a variety of single-purpose products. Because of this, many of the products suffer from integration problems and missing functionality.

The most complete and integrated of these products is Intel's LANDesk Management Suite 6.0. This suite offers you a set of applications that perform a thorough list of desktop chores, including software distribution and update, network inventory, software metering, and virus protection. The distribution features either let you push new software to desktop clients, or let clients pull the software from a network server. The inventory component lets you keep an eye on how individual desktop machines are configured, which helps when planning migrations and upgrades.

The product can also perform some server management tasks, such as software and hardware inventory and server monitoring. In addition, LANDesk lets network managers troubleshoot desktops remotely, using diagnostic, remote control, remote execute, and remote reboot tools, among others.

Ultimately, LANDesk was designed with the enterprise in mind. Along with its comprehensive feature set, it works in mixed NetWare and Windows NT environments, and it can service desktops across a range of platforms, including DOS, Macintosh, OS/2, and Windows 3.x, 95, and NT.

Intel, 2111 N.E. 25th St., Hillsboro, OR 97124, (503) 696-8080 or
(800)
538-3373, www.intel.com.

----- GIGABIT ETHERNET

Foundry Networks

FastIron Backbone Switch

The Gigabit Ethernet market is populated by many products that have divergent feature sets. While one system's cited packet per second (pps) throughput level may be very high, another system may excel in terms of total bandwidth capacity. And, Gigabit Ethernet vendors are claiming layer 2, layer 3, and even layer 4 performance levels for their products, which muddies the waters even more.

Cutting through some of this haze with a dose of good old-fashioned reality is Foundry Networks' FastIron Backbone Switch. The FastIron is a 16-port, layer 2, 10/100 Fast Ethernet system with Gigabit Ethernet uplink ports.

The switch can process 7 million pps, and it supports such features as virtual LANs, port trunking, and quality-of-service mechanisms.

FastIron Backbone Switch stands out because most users aren't going to rip out their existing systems and convert to 100 percent Gigabit Ethernet in one fell swoop. They're going to do it in stages, as time, money, and legacy systems permit.

FastIron's compliance with this reality is worth more than all the hype, hoopla, and information haze that even the most trend-centric industry can drum up.

Foundry Networks, 680 W. Maude Ave., Ste. 3, Sunnyvale, CA 94086,
(408)
731-3800, www.foundrynet.com.

----- ENTERPRISE ROUTER

3Com

CoreBuilder 3500

In the heat of the supposed war between Gigabit Ethernet and ATM, many vendors would have you believe that you need to choose between the two technologies. 3Com's CoreBuilder 3500 gives you the option of supporting both Gigabit Ethernet and ATM on a single router/switch. As a router, the ASIC-based CoreBuilder 3500 can handle IP, IPX, and AppleTalk Phase 2 packets at wire speeds up to 4 million packets per second. Yet the

CoreBuilder's latency specs are more typical of a layer 2 switch--typically between 15 microseconds and 30 microseconds. It is also capable of handling

IP multicast traffic and will ultimately support IPv6.

Aside from Gigabit Ethernet and ATM interfaces, the CoreBuilder 3500 also handles 10/100Mbit/sec Ethernet and FDDI. It supports three methods of defining Virtual LANs (VLANs): an arbitrary collection of layer 2 ports, ports based on particular layer 3 protocols, and ports based on layer 3 addresses. VLAN support also includes 802.1Q tags.

The CoreBuilder also provides several choices for traffic prioritization.

By supporting RSVP, advanced queuing methods, and 3Com's PACE (a proprietary multipath technology), the product can offer class-of-service definition and quality-of-service policies over frame-based media as well as ATM.

It's worth noting that the CoreBuilder 3500 is less costly than products that are positioned as "layer 3 switches," and, of course, is much less costly than traditional multiprotocol routers.

3Com, 400 Bayfront Plaza, Santa Clara, CA 95052, (408) 764-5000 or (800) 638-3266, www.3com.com.

----- WORKGROUP ROUTER

Ascend Communications

Pipeline 75

If you want to share ISDN connectivity with a small group of users, you can't beat Ascend's Pipeline 75. (The Pipeline 75 is identical to the Pipeline 50, except that the 75 includes two plain old telephone system jacks so that you can connect analog telephones or fax machines.) The

Pipeline 75 can route IP, IPX, and AppleTalk, and it can serve as a bridge for any protocols it doesn't route. It can be configured for "nailed up"

ISDN or for frame relay, as well as for ordinary switched ISDN service. It can serve as a firewall with an extra-cost option.

It might not be fair to say the Pipeline 75 is easy to configure--no router is easy--but Ascend provides a Java-based QuickStart utility that makes it easy (relative to comparable routers). The fact that Ascend routers are widely used by ISPs means that there is plenty of expertise if you get stuck.

Aside from the graphical Java-based configuration console, you can also configure the Pipeline over Telnet or via a serial port with a straightforward text menu interface. In addition, there is a command line interface for serious router types. Remote configuration and monitoring is a breeze.

The difficulty of setting up ISDN is overemphasized. In fact, the telephone company or ISP provides users with a handful of simple parameters, making it relatively easy to set up ISDN. Incorporating multiprotocol bridging and routing into a corporate network is a bigger challenge, and Ascend does a fine job of simplifying the task.

Ascend Communications, One Ascend Plaza, 1701 Harbor Bay Pkwy., Alameda, CA 94502, (800) 272-3634, www.ascend.com.

----- ENTERPRISE SWITCH

Bay Networks

Accelar 100

As the line between switching and routing blurs, a crop of hybrid

terms such as routing switch, switching router, and switch/router has sprung up.

Factor into this equation the emergence of multilayer systems, and you've got a real semantic stew brewing.

Living up to these labels is no easy task. In the case of an enterprise system, it means delivering very high throughput rates with very low latency, as well as performing the maximum possible number of routing functions.

The important distinctions between these functions are beginning to manifest themselves in products. Bay Network's Accelar 100 routing switch, for example, functions at both the layer 2 and the layer 3 levels. Its architecture separates data traffic and controls traffic by using two 1.2Gbit/sec buses. The Accelar 100 also forwards packets from client ports in a balanced fashion--a major stride in avoiding congestion problems.

The Accelar 100 was designed not as a replacement for traditional routers, but as a sort of "booster" system. It's based on a distributed switching architecture through which IP and IPX forwarding are performed at layer-2-switch latencies. The system can also interface with existing routers using legacy protocols such as AppleTalk and DECnet, so it doesn't require a forklift upgrade to be integrated into existing networks.

The Accelar 100 also includes quality-of-service features via priority queuing, and support for IP multicast.

Bay Networks, 4401 Great America Pkwy., Santa Clara, CA 95054, (408) 988-2400, www.baynetworks.com.

----- WORKGROUP SWITCH

SMC Networks
TigerSwitch 100

Today's networks are starving for additional bandwidth, and there's an increasing number of ways to feed this need. In fact, the menu of options to choose from seems to grow almost daily.

But when it comes to pushing packets, there is such a thing as too much, too soon. Before you implement a drastic change geared toward expanding your network pipe, it's important to ensure that you can handle the increased data flow it can deliver. Otherwise, you're faced with the possibility of excessive collisions, traffic jams, or even total network meltdowns.

Enter the 10/100 switch, which helps to smooth the transition to higher-speed technology. SMC Networks' TigerSwitch 100, a Fast Ethernet workgroup switch, is a worthy standout in equipment that can provide the additional bandwidth needed--without a major infrastructure overhaul. The system also enables users to integrate Fast Ethernet in stages.

The TigerSwitch has eight auto-negotiating 10/100 ports, which serve as a sort of "performance police." Also, the system is based on a nonblocking architecture, has 1.8Gbits/sec of internal bandwidth, and includes Spanning

Tree support.

The TigerSwitch 100 also includes SMC's SNMP package, called EliteView for

Windows. An added bonus is a wide array of status LEDs on the front panel, which maintains updates on data rate, collision and forwarding activity, and utilization and diagnostic statistics, among other indicators.

SMC Networks, 350 Kennedy Dr., Hauppauge, NY 11788, (800) 762-4968, www.smc.com.

----- FIREWALL

CheckPoint Software Technologies
Firewall-1 3.0

The firewall market is still experiencing a glut of products, all claiming to be the most secure first line of defense for an enterprise network.

Sifting through the dozens of products can be maddening, but there is one that's still the best. CheckPoint Software's Firewall-1 was the early

favorite in the firewall marketshare race, and although many other companies are trying to eat into its piece of the pie, CheckPoint continues to beef up its product, so it's second to none.

The company's Stateful Inspection architecture leads the way in features that make this product truly innovative; in fact, many other vendors are using this technology in their products.

Firewall-1 intercepts incoming packets at the Network layer, where the

Stateful Inspection engine takes over and extracts relevant data to determine if the packet conforms to the defined security policy. Only then can the packet be processed by higher layers in the protocol stack.

Besides putting up a strong front door, Firewall-1 also includes virtual private networks capability by supporting encrypted sessions between firewalls or between a secure client and a firewall.

The 3.0 version includes support for several secure Internet protocols, including Internet Protocol Security (IPSec), simple key management for

Internet protocol, and Manual IP. Not to be overlooked is the speed with which Firewall-1 can examine packets and the ease with which new services can be added.

Rather than follow the adage, "Don't mess with a good thing,"

CheckPoint has gone ahead and done nothing but improve upon its good thing.

Check Point Software Technologies, 400 Seaport Ct., Ste. 105, Redwood City,

CA 94063, (650) 482-4900, www.checkpoint.com.

----- INTRUSION MONITORING

Internet Security Systems

RealSecure 1.0

Firewalls are absolutely essential for keeping intruders out of your network, but if someone were to attempt a break-in, how would you know? A relatively new category of products that act as sentinels for your network resources has started to gain recognition, and a star in this crowd comes from Internet Security Systems.

RealSecure 1.0 makes use of a distributed architecture with attack monitors placed at various points on your network. If an attack is recognized, the administrator is alerted via e-mail and an alarm is sent to the management console. The event is logged, and RealSecure can even terminate the attack automatically. Additionally, the attack can be recorded and later played back (for example, as criminal evidence).

The product is designed to complement firewalls and other barriers to intruder entry. Putting a firewall in place is a wise and necessary precaution, but how can you be sure that your defense is completely effective? RealSecure is designed to let you know (in real time) about such security breaches.

RealSecure's attack-recognition database covers a wide variety of network attacks. For example, the software can spot Satan scans, denial-of-service attacks, and several types of attacks on the Windows OS (such as unauthorized attempts to access a Windows network share, unauthorized attempts to access a Windows registry remotely, or unauthorized attempts to access a Windows password file).

Internet Security Systems, 41 Perimeter Ctr. E., Atlanta, GA 30346, (770)

395-0150, www.iss.net.

----- PROXY SERVER

Novell

BorderManager

It used to be that a good proxy server would cache frequently accessed Web pages, block access to predefined URLs, and serve as a central point for internal end users to pass through on their way to the Internet. How things have changed in the last year.

Now, to distinguish one proxy server from another, companies are adding features that almost make the label proxy server obsolete. Novell has taken this product niche and gone many levels above what anyone else is

doing.

Yes, Novell BorderManager features FastCache, which will load pages up to

200 times faster than going out across the Internet to the remote site will, but this is only the beginning of Novell's offering.

BorderManager also includes network address translation support, which eliminates the need for each internal client to have a unique IP address, while at the same time conceals internal IP addresses from the outside world. It also includes some firewall capabilities, an IP/IPX gateway, and even some virtual private network features.

Tight integration with Novell Directory Services (NDS) is one of BorderManagers most attractive features, allowing administrators to keep all users under the same tree.

So you say you're not a Novell shop? There's no need to worry because BorderManager comes with a two-user license for IntranetWare 4.11.

BorderManager is one step in Novell's much-anticipated foray into the world of Internet technologies, and from the looks of things, the company's doing just fine.

Novell, 122 E. 1700 S., Provo, UT 84606, (801) 861-7000, www.novell.com.

----- CERTIFICATE TECHNOLOGY

ValiCert

Validation Server

Digital certificates are being hailed as the answer to securing communications over the Internet--from authenticating Web site access, to ensuring the integrity of e-mail messages, to verifying credit card authorization in e-commerce transactions. However, a hidden obstacle in the system could hinder the efficiency of certificate systems.

The problem lies in Certificate Revocation Lists (CRLs), which are records of invalidated certificates. When a certificate is revoked, it is recorded on a CRL. If a server has not yet received an updated CRL, a window for misauthentication exists. And, as the number of certificates in use grows, so will the number of CRLs, along with the burden of managing them.

One product has emerged that addresses CRL management. The ValiCert Validation Server allows real-time CRLs checks, and provides an orderly method of maintaining CRLs via certificate revocation trees.

An organization using a certificate system can set up a ValiCert server as the main warehouse for CRL information. When a user requests access to a network resource, a certificate server can check the request against the

ValiCert server in real time. Because the CRL data is centrally stored, network managers can be sure that certificate servers have access to up-to-date CRL information. Also, central administration makes managing CRL data easier for the network manager to facilitate.

ValiCert, 3160 W. Bayshore Rd., Palo Alto, CA 94303, (650) 849-9860, www.valicert.com.

----- AUTHENTICATION

CyberSafe

TrustBroker Security Suite (formerly Challenger)

Networks tend to grow in piecemeal fashion, and network security is no different. However, the central issue in network security is controlling who has access to the network across the board.

CyberSafe's TrustBroker Security Suite, the newest incarnation of the Challenger product, avoids having to stitch together a security strategy by offering a robust and flexible security platform that provides end-to-end, enterprise-level access control.

The key to TrustBroker's strength is its flexibility. The product, which is based on Kerberos and public key technology, lets you build a cohesive security system by using various technologies to suit your unique networking environment. For instance, using the single sign-on component, you can provide users with a basic means of authentication to multiple network resources. If you need more strength or want to secure a specific

portion of the network, TrustBroker supports token card technology. To secure remote users, you can extend TrustBroker with its Remote Dial-Up package. Another aspect of its flexibility is the wide range of platforms it supports, from Unix and Windows 95 and NT, to Macintosh clients.

Aside from authentication, TrustBroker also provides related secondary security, including encryption, message integrity, password protection, and mutual client-to-server and server-to-client authentication. And, CyberSafe is developing additional security features, including secure Web agents.

CyberSafe, 1605 N.W. Sammamish Rd., Issaquah, WA 98027, (425) 391-6000, www.cybersafe.com.

----- ENCRYPTION

Sun Microsystems

SunScreen SKIP

The value of firewalls and authentication systems is a no-brainer for anyone designing a network. But to prevent anyone else from getting their roaming eyes on your data, especially as it crosses the public Internet, you need a solid encryption package that will safeguard all IP applications without having to modify the applications themselves.

SunScreen SKIP will do the job whether you're using Windows 95 or NT, or

Sun Microsystem's own Solaris operating system. The product not only encrypts all IP traffic traversing between clients, but, through support of signing keys and digital certificates, also confirms the integrity of that information by ensuring it hasn't been tampered with or looked at by others. (SKIP supports such encryption algorithms as Data Encryption Standard [DES] and RC4.)

By operating at the Network layer, SunScreen SKIP is independent of application, which means it can secure all TCP and UDP applications without those applications having to know anything about what's going on.

Export of encryption products has been a volatile topic between vendors and various national governments, so Sun has worked out a clever compromise.

U.S. and Canadian customers can purchase a 2,048-bit version of the product, while others can choose from 512-bit and 1,024-bit versions, depending on what's allowed in their country.

SunScreen SKIP interoperates nicely with Sun's SecureNet products, which provide firewall and authentication capabilities, but the product works on its own, too, making it a sound investment for companies that don't want their business turned into public knowledge.

Sun Microsystems, 901 San Antonio Rd., Palo Alto, CA 94303, (650) 960-1800 or (800) 786-7638, www.incog.com.

----- NETWORK ANTI-VIRUS

Computer Associates' Cheyenne Division

InocuLAN 4.0

When it comes to virus detection capabilities, there really isn't much separating top shelf network anti-virus products. They all do what they're supposed to do. What really distinguishes one product from another is its management and administration features. These "extras" are what set InocuLAN 4.0 apart from the competition.

InocuLAN eases network administration through Windows-based domain grouping of servers and workstations, and the NetWare version is integrated with

Novell Directory Services (NDS). A new feature lets administrators remotely install InocuLAN clients from the server. InocuLAN also features Scanning

Logs, which show the complete virus scanning history for a workstation, domain, or network, including files checked, viruses found, and responses taken.

InocuLAN also automates many of the tedious, time-consuming installation and management tasks. It features Hands-Free Updating, which automatically dials, downloads, and updates all InocuLAN servers and workstations with the latest virus signature update files; it even

automatically uploads and reloads itself on the server. InocuLAN scans can be scheduled to run automatically during low-traffic periods to reduce system load.

InocuLAN can detect and cure 100 percent of viruses in the wild, and it can identify and isolate programs that exhibit virus-like behavior.

Additionally, InocuLAN servers can be set to automatically download and distribute monthly updates of virus signature files from Cheyenne's BBS,

Web site, and CompuServe forum.

Computer Associates, One Computer Associates Plaza, Islandia, NY 11788,
(516) 342-5224, www.cai.com.

----- REMOTE ACCESS

Shiva

LanRover Access Switch

If you asked a group of network managers who among them is not supporting remote users, scarcely a hand would go up. The reality today is that small and large companies are supporting remote offices, mobile workers, and telecommuters, while trying to provide them the same service, reliability; and security as network-attached users.

In comes Shiva, and the product that's now won this category two years running, to save the day. The LanRover Access Switch is exactly what enterprises need for allowing a multitude of different connections in one box without the complications of many enterprise-level remote access products on the market:

If you have ISDN, T-1, and analog modems, the LanRover Access Switch can handle all of them. In fact, a single telephone number can support analog and ISDN access from one or more PRI lines.

The product can also support just about every client platform you can think of; and installation and management are a snap as well. And, to ensure that only authorized users ever get authentication, the Access Switch supports password authentication protocol and Challenge Handshake Authentication

Protocol (CHAP).

For companies that feel they have no control over rising telecommunications costs, the LanRover Access Switch includes Shiva's Tariff Management, which provides services like bandwidth-on-demand; the product can also end a call when data stops flowing over a line.

Shiva was one of the earliest entrants into the remote access market, and it continues to provide feature-packed products for enterprise users.

Shiva, 28 Crosby Dr., Bedford, MA 01730, (781) 687-1000,
www.shiva.com.

----- WIRELESS NETWORKING

RadioLAN

Wireless BackboneLink

When most people think wireless, "warp speed" typically isn't the first term that comes to mind. This relative sluggishness is one factor that's held the technology back in many cases. Were it not for this limitation, wireless would have likely gained a stronger foothold for applications such as remote access. Instead, it's the traditional wired networks that have been relied upon to deliver, closing off some potential opportunities for wireless technology.

However, one major stride in speed has been made by RadioLAN's Wireless

BackboneLink. This standalone bridge links the company's wireless systems with standard wired 10Mbit/sec Ethernet networks. The system can also serve as a wireless-only network in an organization's branch offices.

The Wireless BackboneLink has one 802.3-compliant wired interface and one

RadioLAN wireless interface. The system can accommodate up to 128 users per access point, and laptop users can move from one BackboneLink to another and still remain connected to the network at the full 10Mbit/sec speed. The

Wireless BackboneLink also supports the IEEE 802.1d Spanning Tree protocol, as well as filtering by source or destination address or by protocol.

The system includes RadioLAN's RadioNet Backbone Manager software, which enables configuration of IP address and subnet masks via DHCP.

The software enables the user to perform tasks--such as discovering of network connections automatically, accessing configuration utilities, and configuring user names and passwords--from any location on the network.

Radiolan, 455 DeGuigne Dr., Sunnyvale, CA 94086, (408) 524-2600, www.radiolan.com.

----- TELEPHONY GATEWAY

VocalTec Communications

Telephony Gateway 3.1

Telecommunications monopolies come and go, and we still complain about the cost of making a long distance telephone call.

But as IP became the ubiquitous WAN connection for many companies, the idea of running voice over this relatively cheap infrastructure made IP telephony one of the hottest buzz words of 1997.

The company that blazed the way into this new frontier is VocalTec, which many know from its Internet Phone product, which allows customers to call far-flung relatives and pay for only a local call.

VocalTec took that innovative idea one step further and created the Telephony Gateway, which allows businesses to use the Internet for carrying phone calls throughout the world.

Through either a phone or PC, users make a local phone call to the gateway, which then communicates over IP with another gateway near the call recipient's location. The other gateway then either communicates directly with a computer on the other end, or goes through the local PSTN to a regular phone.

One of the attractive qualities of Telephony Gateway is its ability to reduce the bandwidth necessary for a single phone call from the traditional

64Kbits/sec to around 8Kbits/sec to 10Kbits/sec, making it possible to run many more simultaneous calls over the same link.

The product runs on a Windows NT 4.0 Pentium machine with Dialogic boards and takes very little time to install.

Rather than attempting to replace the traditional telephone network that has been providing reliable service for a century, VocalTec's Telephony

Gateway brings a choice to the confusing and sometimes monopolistic world of telephone communication.

VocalTec, 35 Industrial Pkwy., Northvale, NJ 07647, (201) 768-9400, www.vocaltec.com.

----- VIDEO CONFERENCING

PictureTel

LiveLAN 3.0

PictureTel continues to lead the video conferencing market, as it has for some time, in delivering the clearest audio and video you will find.

Previously, corporations that desired video conferencing were stymied by

ISDN restrictions. Now H.323-compliant products, such as LiveLAN 3.0, can broadcast high-quality audio and video over any network transport that supports TCP/IP, such as Ethernet, Fast Ethernet, FDDI, Token Ring, frame relay, and ATM, without any modifications to the existing LAN infrastructure.

LiveLAN 3.0 includes a video conferencing board, camera, speakers and microphone, and T.120 multipoint collaborative computing software. The collaboration software is another feature that sets LiveLAN apart from its competitors. Besides being easy to use, data transfers occur in real time.

Applications include file transfer, white board, and remote control. The

LiveLAN client for PCs runs on Windows 95.

The product includes LiveGateway, a bidirectional gateway that

enables conferencing with H.320 video conferencing products (those that connect over ISDN), and LiveManager, a conference management software application.

If the bandwidth demands incurred by video conferencing are a concern,

LiveManager can help manage them. It lets you monitor and dictate, on a segment-by-segment basis, the amount of bandwidth that is allocated for

LiveLAN calls throughout the network.

Another bonus that comes with using a PictureTel product is the number of comprehensive suites available. The variety of PictureTel solutions allows corporations the flexibility and scalability for mix-and-match environments.

PictureTel, 100 Minuteman Rd., Andover, MA 01810, (978) 292-5000 or (800) 716-6000, www.picturetel.com

----- WEB SERVER

Apache HTTP Server Project

Apache Web Server 1.2.4

With the explosive growth of the Internet over the past four years, it's not surprising to see a parallel growth in the Web server market--as well as the marketing war.

When the dust began to settle, there seemed to be a forgone conclusion that the proliferation of server choices would quickly narrow itself to one or two from the heavy hitters. Consumers anticipated they would have to choose between paying for their server out-of-pocket and obtaining it for free and conforming to networking or application standards that run counter to the open environment of the Internet's infancy.

The free Apache Web Server has confounded nearly every pundit's projection since it was introduced in December 1995. Initially based on NCSA's HTTP

Daemon 1.3, Apache was literally patched together by a consortium of Web masters who wanted to add functionality to, or repair bugs in, NCSA's existing software.

The initial cooperative seed quickly sprouted into a consortium of contributors who share in the development and management of the project.

The result? A robust, stable, extremely inexpensive, and constantly upgraded product that dominated the web server market a year after its introduction and which continues that domination to this day. The Apache source code is freely downloadable from the Apache Web site, as are a variety of standard, precompiled configurations. It runs on most varieties of Unix, as well as

Windows NT and OS/2.

Apache Web Server Project, www.apache.org.

----- LOAD BALANCING HARDWARE

RND Networks

Web Server Director

TCP/IP load-balancing hardware distributes traffic over multiple Web servers by measuring round-trip server response times and redirecting traffic to the server that can best handle incoming requests. It provides

Web administrators with an alternative to expensive server upgrades if they need to improve their site's overall performance and reliability.

The main drawback that these products present has been that responses must be rerouted back through the load-balancing server, making them inappropriate for configurations that include remote servers--that is, this has been a limitation until now.

The Web Server Director family of products, consisting of WSD, WSD Pro, and

WSD-DS (intended for distributed sites), provides a scalable solution that can balance across local servers and remote sites. This makes it ideal for

ISPs or large networks that can't tolerate a single point of failure. Furthermore, the WSD products are competitively priced, ranging from under

\$8,000 for WSD to \$22,500 for WSD-DS, compared to a high of \$32,000 for its competitors. Three product levels, distance-based redirection, and competitive pricing make the WSD family an ideal choice for administrators who wish to take advantage of the benefits of load balancing while retaining the option to scale the size and complexity of their Web environment as their sites grow.

The Intel Pentium-based WSD units offer 90Mbit/sec throughput and support up to 900,000 concurrent TCP/IP connections, guaranteeing that you'll probably run out of bandwidth before you overload your load balancer. WSD,

WSD-DS, and WSD-Pro support 100, 1,000, and 50,000 virtual servers, respectively.

RND Networks, 3505 Cadillac Ave., Ste. G5, Costa Mesa, CA 92626,
(714)

436-9700, www.rndnetworks.com.

----- ENTERPRISE WEB MANAGEMENT

Bright Tiger Technology
ClusterCATS

Load balancing hardware and software increase Internet or intranet performance and availability by measuring response times from two or more servers and directing traffic to the one with the highest availability.

While this solution improves performance and provides fail-over for a Web site, an emerging breed of tools goes a step further to help manage the distribution of resources and the flow of traffic over your network.

The first comprehensive Web management solution to make it to market was

ClusterCATS. Its three components, which include Server, Observer, and

Explorer, combine load balancing, content and application distribution, distance-based traffic redirection, and centralized management and monitoring into one powerful management solution.

What sets ClusterCATS apart from its competitors is its global approach to managing and monitoring every component in the Web environment. This includes content, applications and transactions, servers, and the network.

In addition to directing traffic to the best server based on distance or response times, it lets Web administrators actively allocate and distribute resources on multiple servers throughout the Web environment.

Once these resources have been allocated, ClusterCATS' Publish and Subscribe feature automatically synchronizes and updates content throughout the network servers. ~~ClusterCATS can be scaled~~ from small Web hosting applications running a pair of virtual servers to geographically dispersed intranet applications.

Bright Tiger Technologies, 125 Nagog Park, Acton, MA 01720, (978) 263-5455, www.brighttiger.com.

----- VALUE-ADDED ISP

MCI Telecommunications

ISPs are redefining the "service" in Internet Service Provider. They are developing products and adding options to their current list of services in the hope of becoming invaluable partners with their customers. MCI is leading the way with a variety of value-added services. Customers can order a site analysis (which includes an inspection of the customer's network), as well as equipment installation and monitoring. Connection options include 56Kbits/sec to T-1, multiplexed T-1s, fixed rate DS-3, and full rate DS-3.

For companies that don't want to manage a Web site, MCI provides Web design services, Web and FTP hosting, and database hosting of Microsoft SQL on

Windows NT, Informix, Oracle on Windows NT or Unix, and Sybase.

For clients venturing into electronic commerce, transaction processing is available. For Web sites that require multimedia, MCI offers RealNetworks products for audio and video streaming. Customers can obtain InterNIC domain name services through MCI, and MCI will host the mail

server. Data and voice virtual private networks are also available.

MCI supports these offerings with a strong OC-12 (622Mbit/sec) backbone that reliably delivers the services it offers. The company also provides

24-by-7 technical support. If something does go wrong, MCI offers service agreements on a case-by-case basis, depending on the customer's applications. A 90-minute outage accrues a one day credit; three-hour outages yield a week of credit.

MCI Center, Three Ravinia Dr., Atlanta, GA 30346, (770) 280-6000, www.mci.com

----- ISP WORLDWIDE SERVICE

UUNET Technologies

When searching for an ISP with worldwide coverage, a variety of access options, and high customer satisfaction, UUNET tops the chart. With 10 years of experience under its backbone, UUNET has created a network with

400 POPs in the United States and 550 international POPs throughout the world. UUNET reaches all the major network access points and provides 100 percent coverage in the United States.

Plus, the backbone is expanding. In the last couple of years, the company spent \$300 million to upgrade parts of its network backbone to OC-12

(622Mbits/sec).

Another nice feature from UUNET is its coverage to business customers. It isn't sidetracked trying to please or entice consumer business. With this business-focused philosophy, the company has amassed more than 70,000 customers who can choose frame relay, SMDS, ATM, OC-3, T-1, T-3,

56Kbit/sec, ISDN, or xDSL connections. The network is fully redundant at every link, and a UPS is located at every switch point. If a link fails, traffic is rerouted automatically without loss of service. The network operating center, located in Fairfax, VA, is staffed around the clock and has at least one senior engineer on the site at all times.

UUNET backs up its service with service-level agreements in its contracts; if service is not provided above a certain percentage, UUNET gives a rebate to the customer.

UUNET Technologies, 3060 Williams Dr., Fairfax, VA 22031, (703) 206-5600, www.uu.net.

----- ELECTRONIC COMMERCE

InterWorld

Commerce Exchange 2.0

You can't run critical business applications in an enterprise environment with bargain-priced products. In accepting the axiom that you have to spend money to make money, Commerce Exchange is the clear leader in its field.

Commerce Exchange is aimed at customers who have more than 50,000 transactions per year and over \$2 million in annual online sales. It automates sales and distribution cycles from the initial order to the final delivery, and it can minimize or eliminate credit card verification, inventory management, security, billing, accounting, and customer service functions.

As if that weren't enough, it also integrates with legacy systems without very much fuss. It links to Oracle, Sybase, Informix, and SQL Server databases, plus Netscape and Microsoft Web servers. Additionally, it runs on Unix or Windows NT and uses Secure Sockets Layer (SSL) and RSA encryption.

One item that sets Commerce Exchange apart from its competitors is that it batches transactions in real time. Another key aspect of this product is its ease of use; rather than sucking precious IT resources, it can be used and managed by someone in the sales or marketing department.

Commerce Exchange can also be used to personalize customers' visits based on buyers' past history, and it processes payments using CyberCash. With a starting cost of \$75,000, this solution does not come cheap, but it's worth every penny.

InterWorld, 395 Hudson St., Sixth Fl., New York, NY 10014, (212)
301-2500, www.interworld.com.

----- STORAGE MANAGEMENT

Computer Associates

ARCserve 6.5 Enterprise Edition

The best is better. Last year, we awarded Cheyenne (a division of
Computer Associates) our Product of the Year for ARCserve 6 for NetWare and
Windows

NT. For this year's awards, we looked at all the alternatives, and
found that the upgraded ARCserve 6.5 Enterprise Edition, available for
Windows

NT, is king of the hill.

What do we like? Well, we like that a single console can manage
multiple machines, running not only Windows NT, but also OS/2, Macintosh,
Unix, and

NetWare. We like that the client decides what is "pushed" to the
ARCserve host server (in other words, that security is maintained). We were
also impressed with ARCserve's support for remote installation and client
administration, making it ideal for large enterprises.

ARCserve also supports a huge range of backup devices, from 100Mbyte
media such as Iomega's Zip drive to ATL Product's Series 2640 DLT Library
(see

"Archival Storage"), and can provide RAID 5-like data striping across
multiple tape devices. It can even back up to MVS mainframes. The new

ARCserve 6.5 offers even more functionality, such as the use of an

ODBC-compliant database instead of ARCserve's native database,
prioritization of backup sources, support for Informix and OpenIngres, and
end-to-end data compression and encryption. The newest twist is that

ARCserve includes the Unicenter TNG Framework (see "Management
Platform," page 33), giving it tremendous capabilities for auto-discovery,
virus scanning, job scheduling, sophisticated alerts and reports, and more.
Now this is what storage management is all about.

Computer Associates, One Computer Associates Plaza, Islandia, NY
11788,

(516) 342-5224, www.cai.com.

----- HIGH-AVAILABILITY SYSTEM

NSI Software

Double-Take

Inaccessible e-mail, Web site crashes, and downed transaction
processing systems--any of these failures, and the ensuing hours of data
recovery and lost revenue, could cost your company thousands, or even
millions, of dollars. To avoid such costly disasters, you need a system
that is capable of providing both high availability and data protection for
your critical systems.

Enter NSI Software's Double-Take, a high-availability solution that
combines real-time data protection with automatic server failover to
eliminate, or significantly reduce, downtime and data loss.

While other data-protection/high-availability products offer similar
functions, Double-Take stands out in its support for multiple platforms--a
critical requirement in many enterprise environments. The software is
currently available for both Windows NT and NetWare, and a Solaris version
is in the works. Adding to Double-Take's appeal is its support for multiple
configurations--one-to-one, one-to-many, and many-to-one--on all platforms.

Operating at the file system level, Double-Take replicates selected
data or entire volumes from source servers to target servers across LAN and
WAN links. Should one or more source servers fail, the target server
assumes the failed servers' names and IP addresses automatically, allowing
users to continue accessing data without interruption.

Because it can operate over WAN links, Double-Take is suitable for
providing disaster recovery protection. Source servers can link to an
offsite server, sending continuous updates of critical data over the WAN
link. And because the software sends only modified portions of files, it

minimizes bandwidth consumption across slow WAN connections.

Double-Take can also be used to centralize backup at a target server, and to create accurate and current test environments, where relevant files and directories are copied to a test server.

With its cross-platform support, multiple configuration options, and myriad applications, Double-Take addresses your most critical data protection and highavailability needs.

NSI Software, 80 River St., Ste. 5B, Hoboken, NJ 07030, (630) 357-8110 or
(888) 230-2674, www.nsisw.com.

----- SERVER STORAGE

Storage Dimensions

SuperFlex 5200

When it comes to server storage, it seems Storage Dimensions just can't be beat. Last year we recognized the company's SuperFlex 5000 as the best server storage system on the market. This year, we're tipping our hats to the SuperFlex 5200, which builds upon the 5000's superior technology to deliver the best performance and reliability for mission-critical Windows

NT, NetWare, and SunSPARC servers.

Doubling the capacity of the 5000, the SuperFlex 5200 contains 14 drive bays, which house 4.3Gbyte, 9.1Gbyte, or 18.2Gbyte UltraSCSI 7,200 rotations-per-minute disk modules. And, like its predecessor, the system lets you create up to eight logical drives, each with its own RAID level, giving you the flexibility to address different application needs.

With its redundant RAIDFlex-D SCSI-to-SCSI array controllers, the SuperFlex

5200 delivers superior performance and reliability. Each controller contains an i960 RISC processor, which off-loads RAID operations from the server CPU and improves I/O performance. The two cache subsystems provided by the controllers let you scale write-through cache from 32Mbytes to

128Mbytes, which can significantly enhance performance, depending on application and workload. When configured with two host bus adapters, the

5200 can reach peak transfer rates of 40Mbytes/sec and sustained rates of

30Mbytes/sec.

As for reliability, the dual controllers eliminate a single point of failure; should the primary controller fail, the system automatically switches to the secondary one. The 5200 also supports clustered applications, should you need to implement this level of fault tolerance.

Storage Dimensions, 1656 McCarthy Blvd., Milpitas, CA 95035, (408) 954-0710 or (800) 765-7895, www.storagedimensions.com.

----- ARCHIVAL STORAGE

ATL Products

Series 2640 DLT Library

There are two basic approaches to archival storage. First, you can allocate backup devices and media on a server-by-server basis; this is often the best approach when network bandwidth is limited. However, if you treat your data independently of their servers, which is the second available approach, you can centralize your archival system, making offline storage available throughout the enterprise.

If you opt for the second strategy, you might find that your storage needs are in the terabyte range. Oddly enough, so is ATL Products' Series 2640

DLT Library. This incredible system can contain as many as 264 Digital

Linear Tape cartridges (9.24 terabytes); as many as five libraries can be chained together, yielding an archive of 1,320 tapes (47.7 terabytes) that are treated as a single logical unit. When the five libraries are linked together, tapes are actually passed between units automatically--a fascinating process to observe.

The Series 2640 is more than just a big box with lots of tapes and tape drives. ATL Products has worked with numerous software vendors, including

Computer Associates, Digital Equipment, Hewlett-Packard, IBM, Legato, OpenVision, Seagate software, and Veritas, and claims that nearly 40 major storage management applications--including backup, archive, and hierarchical storage management--can support Series 2640 libraries. ATL, however, hasn't simply left all the software support to third parties; it has two excellent

Java-based offerings of its own. WebAdmin lets users manage the Series 2640 using a Web browser, and WebLibrarian assists administrators in tracking and managing the archival media and content. Altogether, it's a most impressive archival system.

ATL Products, 2801 Kelvin Ave., Irvine, CA 92614, (714) 774-6900, www.atlp.com.

----- NETWORK DESIGN

CACI Products

Comnet Predictor

Network design tools help speed up the task of designing a network by modeling proposed networks to predict network performance. Significant dollars can be lost if mistakes are made in the network design.

Comnet Predictor is an analytical modeling tool that lets you quickly run through several what-if scenarios for possible network designs. Once you've started to zero in on a prospective design, you can then have Comnet

III--CACI's well-known network simulation tool--run a detailed simulation.

Comnet Predictor fills the need for a high-speed analytical tool.

While

Comnet III's detailed simulations are unmatched, running a simulation on a large, complex network could potentially take hours. Comnet Predictor runs an analysis in seconds or minutes (even on large networks). Thus, you can use Comnet Predictor to quickly run through a wide variety of possible network designs. When you've narrowed the field to one or two potential designs, you can use Comnet III for more detailed simulations.

Comnet Predictor shines in its speed, as well as in its ability to keep track of burstiness in the data traffic. Other analytical modeling tools can do much of what Comnet Predictor does, but they don't take into account bursts of data traffic, and they can't catch up to Comnet Predictor's speed.

Comnet Predictor runs on several Unix and Windows platforms, including

HP-UX, IBM AIX, Solaris, Silicon Graphics IRIX, OSF/1 for DEC Alpha, Windows 95, and Windows NT.

CACI Products, 3333 N. Torrey Pines Ct., La Jolla, CA 92037, (619) 824-5200, www.caciasl.com.

----- NETWORK ANALYZER

Network Associates

Sniffer Basic

When your protocol analyzer is part of your desktop (or on a laptop that serves as your desktop), it takes on a very different role than when it's installed on its own computer that has to be connected and booted. The threshold for problems worth the effort of exploration becomes lower, and the tool can be designed to cooperate better with SNMP, RMON, and other sorts of network instrumentation. With the rise of Windows 95 and NT, the dominant platforms support multitasking well enough that it's feasible to perform packet decodes and to display traffic matrices on the same machine that runs your Web browser, word processor, and e-mail client.

The designers of Sniffer Basic did such an elegant job of taking advantage of the Windows environment that Network General acquired the company.

(Sniffer Basic was formerly known as NetXRay. Network General subsequently merged with McAfee Associates to form Network Associates.)

Sniffer Basic comes up with a useful dashboard of monitoring gauges.

However, unlike most other protocol analyzers, it can display a graphical representation of network conversations (as well as a tabular conversation list), sortable by any column, including packets sent, packets

received, bytes sent or received, MAC addresses, or names. Alarms can be triggered by any number of configurable thresholds. Sniffer Basic's packet decodes are presented in an easily grasped form, and all the common protocols, as well as a good selection of esoteric ones, are covered. This is a protocol analyzer package designed to be used day in and day out.

Network Associates, 805 Bowers Ave., Santa Clara, CA 95051, (408) 988-3832, www.nai.com.

----- HOST CONNECTIVITY

WRQ

Reflection for IBM 6.1

It would be easy to imagine that mainframe and minicomputer connectivity products had grown stagnant in recent years--after all, the Internet and the desktop have long been the primary places for exciting products and heavy investment. But host connectivity isn't immune to the rise of TCP/IP and the demand for reduced total cost of computing. WRQ's Reflection for IBM

6.1 is state-of-the-art software that keeps the interface to those legacy applications tuned in to Internet-style rates of change.

Reflection for IBM can emulate 3270- and 5250-type terminals over the Internet. Furthermore, because Reflection supports Microsoft's Active Documents, it can run seamlessly inside ordinary Web browsers, and users can connect to a mainframe application by clicking on a link on a Web page.

Host connectivity normally needs to be installed and managed for numerous users; Reflection provides a great selection of tools for simplifying the lives of administrators and keeping support costs down. Reflection's setup routines make large-scale deployment easy. The Reflection Profiler lets administrators define settings for groups and individuals, as well as control which commands users can change. A special View Settings Dialog displays all settings in one place, and a single mouse click can reset them all to company standard settings.

Reflection for IBM is also fast, outperforming its competitors in data throughput, file transfer speed, and graphics display. WRQ continues to demonstrate a firm commitment to meeting the needs of SNA host users as the computing environment becomes more complex.

WRQ, 1500 Dexter Ave. N., Seattle, WA 98109, (800) 872-2829, www.wrq.com.

----- NETWORK PRINTING

Xerox

DocuPrint N32

Remember the paperless office--that new corporate frontier in which electronic documents would flow effortlessly, without the hassle of hard copies that seem to clone themselves uncontrollably whenever you turn your back?

This vision has yet to become a reality, but the good news is that you don't have to pay a fortune for a fast, versatile monochrome laser printer that can churn out up to 32 pages per minute, as well as collating and stapling multiple copies.

The DocuPrint N32 is one example of Xerox's attempt to muscle in on the

LaserJet 5si Mopier (multiple original printout), Hewlett-Packard's offering that won last year's award in the Network Printing category.

The DocuPrint N32 is essentially based on the same principle as the Mopier:

It's more cost-effective and efficient to print multiple copies of a document straight from the desktop, as opposed to generating a single document and then trudging off to the photocopier to finish off the job.

But Xerox, which is eager to shed its legacy "copier-centric" image, seems to be pulling off this strategy with a smaller price tag. While

Hewlett-Packard's LaserJet 5si Mopier costs roughly \$9,000, the DocuPrint

N32 has a base price of \$2,900. (When you factor in collating, stapling, and various other features, however, the DocuPrint N32 weighs in

at just over \$6,000.)

The DocuPrint N32 also gets high marks in the interoperability column via

PrinterMap, its multivendor printer management software. The software enables users to manage SNMP-based printers from different vendors across the entire network. The alert-driven system lets users track printer usage via a single-view topology map.

Networked printers can be viewed on the basis of attribute, model, or other defined groups, and can be administered through vendor or user-defined groups.

Reports on network printers include information that helps ensure billback to the appropriate device.

Xerox, 800 Phillips Rd., Bldg. 111-01X, Webster, NY 14580, (203) 968-3000 or (800) 349-3769, www.xerox.networkprinters.com.

----- NETWORK FAXING

OMTool

Fax Sr. 2.0

Most network managers would not list faxing as one of the functions of their network, but that may change as a slew of network faxing products establish themselves in the marketplace. Fax Sr. 2.0, from OMTool, is the best of this rapidly improving and expanding field. Fax Sr. allows users to send a fax directly from an application on their desktop, and incoming faxes are routed to the addressee's PC, where they can be viewed, filed, or printed. It also offers integration with major messaging applications, which allows users to send and receive faxes via e-mail.

Besides making faxing more efficient, Fax Sr. makes it less expensive through a feature called Global Routing/Least-Cost Routing. This feature examines and forwards the fax across the network to the office nearest the destination fax machine (a process that is based on its area code and other parameters), saving on telephone line charges.

Certainly, all these features are great, but what really sets Fax Sr. apart are its management capabilities. Fax Sr. allows a network manager to control who can use the fax, where they can fax to, and when they can use it. Fax Sr. can also provide graphs and charts that show system throughput and bottlenecks. It even shows statistics such as how many pages are transmitted per hour and the average time spent sending a fax.

OMTool, Eight Industrial Wy., Salem, NH 03079, (603) 898-8900 or (800) 886-7845, www.omtool.com.

----- EMERGING TECHNOLOGY

Internet Engineering Task Force

Internet Security Protocol (IPSec)

When choosing this year's Emerging Technology of the Year, we had excellent finalists: the H.323 video conferencing standard, thin file servers, embedded HTTP servers, and the Secure Electronic Transaction (SET) standard. But we've chosen the IETF's Internet Protocol Security, or IPSec, as today's most significant emerging technology.

If you look at the IETF's description of IPSec, you wonder what all the fuss is about: "A security protocol in the Network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality." But consider the security problems of using the Internet

(or any IP-based network) for anything more important than surfing www.tvguide.com. Malicious users can spoof IP addresses, making it appear that their evil packets come from a known source; protocol analyzers can eavesdrop on network traffic, and clever programmers can commandeer an authenticated session.

All these problems--and more--can put a damper on Virtual Private Networks

(VPNs), which tunnel private connections over the public Internet. Until IP is secure, VPNs can't be fully trusted. That's where IPSec comes in. The set of protocols, currently an IETF Internet Draft, cover multiple areas, from authenticating packet integrity, to encrypting their contents,

to verifying the identity of a packet's sender, to exchanging keys.

IPSec is hot, and what it will enable will be hotter still once the draft is finalized in late 1998. For more information, check out Anita Karve's tutorial, "Lesson 115: IP Security," either in our February 1998 issue

(page 27) or at www.networkmagazine.com/tutors/9802tut.htm.

Internet Engineering Task Force,
www.ietf.org/html.charters/ipsec-charter.html.

----- SERVER OPERATING SYSTEM

No Award Given

This year, for the first time, we have decided not to recognize a winner in the Server Operating System category.

There is no doubt 1997 was a slow year on the server OS front. Where were the heated battles between NetWare and Windows NT, or between Windows NT and Unix, or between OS/2 Warp Server and anyone? Nowhere, it seems.

That's not to say that server operating systems weren't continuing to evolve and grow, or that they are not vital to enterprises of any size.

IBM's OS/2 Warp Server is metamorphosing into Workspace on Demand.

Microsoft released Windows NT 4.0 Enterprise Edition, with support for an elementary form of clustering. Novell brought out IntranetWare for Small

Business and most of the Unix vendors revved their code.

But there was nothing earth-shattering, nothing that truly made a difference in the state of server operating systems.

What about the future? We see 1998 as pivotal for the server operating system market, as both Microsoft and Novell overhaul their flagship Windows

NT and NetWare platforms, and as RISC Unix purveyors like Sun Microsystems,

IBM, and Hewlett-Packard try to find their home in an increasingly Intel-based world.

But, for now, the envelope is empty.

RELATED ARTICLE: INAUGERATING THE HALL OF FAME

Baseball has its Hall of Fame. So does rock and roll. Why not network product and technology innovators? In the spirit of recognizing not only the best, but firms which are consistently the best, Network Magazine is proud to create our own Hall of Fame, recognizing companies that have won

10 or more of our editorial Products of the Year awards (or have acquired award-winning products or companies). Please join us in congratulating our first five Hall of Fame inductees.

Cisco Systems: 13 awards

(www.cisco.com)

1990 AVS Bridge/Router

1991 AGS+ Bridge/Router, EtherSwitch (from Kapana)

1992 AGS+ Bridge/Router, EtherSwitch (no, it's not a typo-both products won again)

1993 CDDI Adapter Cards (from Crescendo), AGS+ Bridge/Router (yes, again)

1994 Cisco 7000 Router

1995 Cisco 7010 Router, FastLink Switch (from Grand Junction Networks)

1996 Cisco 7500 Router

1997 Catalyst 5000 Switch

----- Hewlett-Packard: 10 awards

(www.hp.com)

1992 LaserJet IIIsi

1993 OpenView

1994 LaserJet 4Si MX, OpenView

1995 SureStore Tape 12000e, OpenView for Windows

1996 LaserJet 5Si/5Si MX, NetServer LS

1997 LaserJet 5Si Mopier

1998 OpenView ManageX (from NuView)

 IBM: 10 awards
 (www.ibm.com)
 1988 Token Ring 16/4
 1991 Notes (from Lotus Development), cc:Mail (from Lotus, which in
 turn acquired it from cc:Mail Inc.)
 1993 Notes 2.1
 1994 Notes 3.0
 1995 LAN Server 4.0 Entry, cc:Mail Mobile/cc:Mail Views
 1996 PC SystemView
 1997 Notes 4.1
 1998 Domino 4.6

 Network Associates: 10 awards
 (www.networkassociates.com)
 1988 Sniffer 2.0 (from Network General), Saber Menu Systems (from
 Saber
 Software)
 1990 Sniffer
 1990 Distributed Sniffer
 1995 SiteMeter 5.0 (from McAfee Associates)
 1996 Sniffer
 1997 Service Level Manager (from Network General), NetCrypto 1.0
 (from
 McAfee Associates)
 1998 Sniffer Basic

 Novell: 13 awards
 (www.novell.com)
 1990 NetWare 386
 1992 NetWare 3.11
 1993 NetWare Management System
 1994 NetWare 4.01, NetWare Connect 1.0, MultiProtocol Router
 1995 NetWare 4.1
 1996 GroupWise 4.1a, Novell Embedded Systems Technology (NEST)
 1997 IntranetWare, ManageWise 2.1
 1998 Novell Directory Services, Border Manager
 COPYRIGHT 1998 Miller Freeman Inc.
 COPYRIGHT 1999 Gale Group
 PUBLISHER NAME: Miller Freeman, Inc.
 EVENT NAMES: *330 (Product information)
 GEOGRAPHIC NAMES: *1USA (United States)
 PRODUCT NAMES: *3573105 (Peripheral Servers (Computers)); 3661251
 (Communications Servers); 3661254 (Bridges/Routers/Gateways); 7372000
 (Computer Software)
 INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office
 Automation)
 NAICS CODES: 334111 (Electronic Computer Manufacturing); 33421 (Telephone
 Apparatus Manufacturing); 51121 (Software Publishers)
 SPECIAL FEATURES: LOB

7/9/56 (Item 21 from file: 16)
 DIALOG(R)File 16:Gale Group PROMT(R)
 (c) 2002 The Gale Group. All rts. reserv.

05665325 Supplier Number: 50127988 (THIS IS THE FULLTEXT)
**Entegrity Solutions Incorporates Digital Certificate Validation Solution
 From Valicert**
 PR Newswire, p629SFM026
 June 29, 1998
 Language: English Record Type: Fulltext

Article Type: Article
Document Type: Newswire; Trade
Word Count: 860
TEXT:

Entegrity Users Will Participate in Field Trial of Global Service

SAN JOSE, Calif., June 29 /PRNewswire/ -- Entegrity Solutions(TM) Corporation, the leading provider of rapidly deployed Public Key Infrastructure-based (PKI) security solutions into the enterprise, today announced that its Security Development Platform (SDP) and Notary Certificate Authority will incorporate cutting-edge technology from ValiCert, Inc. to manage the validation of digital certificates.

Entegrity Solutions' SDP, a standards-based platform for creating security-enhanced applications, is designed to incorporate best-of-breed technologies from multiple vendors as they become available. By embracing industry standards and pursuing cross-certification with other vendors, Entegrity is able to offer the most open security architected platform on the market today.

"ValiCert recognizes the value and convenience of Entegrity's SDP," said Sathvik Krishnamurthy, Vice President of Marketing at ValiCert. "Enterprises, system integrators and application developers now writing to the Entegrity platform can easily SDP-enable digital certificate validation technology into their products."

"With the integration of the ValiCert Universal Toolkit, we have further expanded the power of the platform for our customers. They will now have an easy way to rapidly add validation services to their security-enhanced applications," said John Weinschenk, Vice President of Worldwide Marketing at Entegrity. "The ValiCert Global Service is an added bonus for our large multinational customers with worldwide applications spanning organizational and global boundaries. They will now have a central location to validate their digital certificates."

By integrating ValiCert technology with Entegrity's SDP, revocation data from a certificate system will be sent to a ValiCert validation engine -- either the ValiCert Enterprise Server(TM) (for validating intranet transactions) or the ValiCert Global Service(TM) (for validating extranet/Internet transactions).

Entegrity users will also be able to take advantage of ValiCert's Global Service field trial that involves more than a dozen Certificate Authorities and leading electronic commerce vendors. Through the ValiCert Global Service, enterprises can check the validity of digital certificates across company boundaries and around the world.

In addition, Entegrity customers will have access to other ValiCert products, including:

- * The ValiCert Universal Toolkit' that provides developers with comprehensive off-the-shelf software components for easily building Internet/intranet applications that validate digital certificates using an array of established validation mechanisms.

- * The ValiCert Enterprise Server for creating and issuing verification for digital certificates within an intranet environment, and which provides a link between an intranet and ValiCert's service. The server works with any certificate issuance system to enable high performance, interoperable certificate validity confirmation.

Digital Certificate Validation

Digital certificates are being used increasingly as electronic credentials for identification, payment and other communications and business transactions conducted over the Internet or corporate intranets. As with the credit card industry that developed a way to electronically validate the millions of credit card numbers issued by any bank in the world, the use of digital certificates requires its own clearinghouse network for certificate confirmation so that individuals and businesses can assure the current validity of a certificate.

A pioneer in the emerging area of digital certificate validation, ValiCert's software and services deliver the only universal, high-performance solution available today for validating digital certificates. ValiCert's products and services enable organizations to securely and rapidly manage the validation of digital certificates, and provide enterprise developers and ISVs with the tools to build applications that incorporate certificates.

About Entegrity Solutions Corporation

Founded in 1996 and privately held, Entegrity Solutions is dedicated to ensuring the rapid deployment of secure applications, cost-effectively. The company's product suite, consisting of PKI-based Security Development Platform (SDP), AssureWeb, Notary, AssureMail and Entegrity-SSL, combined with professional consulting services, ensures the integrity of information throughout the enterprise. Entegrity's fully integrated security solutions are deployed in over 12 countries worldwide in a variety of private sector and government projects. Headquartered in San Jose, California, the company's research and development facility is in Sweden, with regional professional services and sales offices in London, Boston, and Washington, D.C.

For more information on Entegrity Solutions, call 408-487-8600 or visit the company Web site at <http://www.entegrity.com>.

About ValiCert

ValiCert was established in 1996 by a group of leading cryptographers and executives from the Internet services industry to build a broad validation infrastructure for the net economy. Utilizing a best of breed suite of technologies, including all traditional methods for certificate validation as well as ValiCert's own innovative cryptographic technique called certificate revocation trees, ~~ValiCert delivers a highly efficient,~~ scalable and transparent solution for checking the validity of digital certificates in any Internet or intranet transaction. ValiCert is headquartered in Palo Alto, Calif. and is available on the World Wide Web at <http://www.valicert.com> or by e-mail at info@valicert.com.

NOTE: Entegrity Solutions and Entegrity are registered trademarks of Entegrity Solutions Corporation. All other trademarks are the property of their respective holders.

SOURCE Entegrity Solutions Corporation

-0-

06/29/98

/CONTACT: Nellie Connors of JONA Group, 415-552-1515, or nellie@jonagroup.com, for Entegrity Solutions Corporation; or Bradley Palmer of Entegrity Solutions Corporation, 408-487-8600, ext. 104, or bradley@entegrity.com/

/Web site: <http://www.valicert.com/>
/Web site: <http://www.entegrity.com/>

CO: Entegrity Solutions Corporation; ValiCert Inc.
ST: California
IN:
SU: PDT

KA-MP

-- SFM026 --

9813 06/29/98 08:03 EDT <http://www.prnewswire.com>

COPYRIGHT 1998 PR Newswire Association, Inc.
COPYRIGHT 1999 Gale Group
PUBLISHER NAME: PR Newswire Association, Inc.
COMPANY NAMES: *ValiCert Inc.; Entegritty Solutions Corp.
EVENT NAMES: *380 (Strategic alliances)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372613 (Network Security Software)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 51121 (Software Publishers)
SPECIAL FEATURES: COMPANY

7/9/57 (Item 22 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

05581786 Supplier Number: 48450598 (THIS IS THE FULLTEXT)

To Drum Up Interest, Valicert Is Giving Away Its Tool Kit

KUTLER, JEFFREY

American Banker, p13

April 28, 1998

ISSN: 0002-7561

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 609

TEXT:

Hoping to put some added momentum behind its digital certification tool, Valicert Inc. is offering its customers more options at a lower price.

Free, to be exact.

The Palo Alto, Calif., company announced the release last week of version 2.0 of its tool kit, which software developers can use to test for certificate revocation within electronic commerce programs.

Valicert contends that digital certificates, the electronic credentials that can verify buyers' and sellers' identities on the Internet, will reach their potential only if accompanied by a highly effective means of ascertaining that a given certificate has not expired or otherwise been revoked.

By giving away its software-it can be downloaded from the valicert.com Web site-Valicert is following a high-tech precept for stimulating market development. That could lead to sales of higher-end products for implementing certificate validation. "Getting the tool kit out develops ubiquity and a PKI," or public key infrastructure, Yosi Amram, the company's president and chief executive officer, said in an interview.

In theory, as on-line commerce and associated certificate volumes expand, system operators would then want to buy the high performance levels of Valicert's server system. Or a company validating certificates across business units might turn to Valicert's service bureau.

While the free distribution may be the main attention-grabber, Valicert may be making an even more significant gesture by rendering its tool kit "universal." It will support any validation protocol and not just the "certificate revocation tree" that Valicert champions.

The 2.0 tool kit thus will accommodate certificate revocation lists, or CRLs, which Valicert has dismissed as a slow legacy technology that will not stand up to the stresses of high-volume commerce. Valicert will also support OCSB, the On-line Certificate Status Protocol, being developed under the auspices of the Internet Engineering Task Force.

Any application developer, whether working on secure virtual private networks or the MasterCard-Visa SET payment protocol, "can use our tool kit to check the validity of any certificate, regardless of the platform they support," Mr. Amram said.

The openness "reflects our ongoing commitment to meeting developers' needs today and in the future for multiple validation and revocation technologies," the Valicert CEO added.

Mr. Amram said legacy systems will have a "clear migration path" to

certificate revocation trees or beyond. He views the more elaborate OCSB as "right for high-value financial transactions" such as wholesale wire transfers, where people will be willing to pay a price, including a delay in response time, for a desired level of assurance.

"We have a system of roads that support Ferraris, Chevys, and buggies," he said. "For validation we need the equivalent. For some very high percentage of transactions-I don't know if it is 92%, 95%, 98%-certificate revocation tree is right."

Mr. Amram said market feedback since Valicert started selling its systems last year was favorable, but there was reluctance to "get on the bandwagon of a proprietary solution. "Now anyone has an easy, free, no-risk tool that is open and universal, supporting any protocol."

"Any tool kit has to embrace whatever method is being embraced by the marketplace for revocation management," said Victor Wheatman, an analyst with the Gartner Group of Stamford, Conn. "Valicert is continuing and extending its strategy of addressing revocation management, and the addition of protocols is appropriate."

The move won praise from the Financial Services Technology Consortium, the cooperative research organization of major U.S. banking companies. FSTC president Adam Backenroth of Chase Manhattan Corp. said it "demonstrates the true interoperability that is crucial for the global adoption of electronic commerce in the banking and financial services industry."

Copyright c 1998 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1998 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *Valicert Inc

EVENT NAMES: *340 (Product specifications)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372000 (Computer Software)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: LOB; COMPANY

7/9/58 (Item 23 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

05475193 Supplier Number: 48297479 (THIS IS THE FULLTEXT)

Warning: Is Your CRL Up-to-Date? Digital certificates hold promise, but managers must monitor revocation status

Kerstetter, Jim

PC Week, p3

Feb 16, 1998

ISSN: 0740-1604

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Tabloid; General Trade

Word Count: 697

TEXT:

IT managers planning to deploy digital certificates as part of their public-key architecture should be warned that poorly managed, revoked digital certificates are a potential security threat.

It's such a threat that VeriSign Inc., Microsoft Corp., Netscape Communications Corp., ValiCert Corp., GTE CyberTrust Inc. and Entrust Technologies Inc. are among the vendors scrambling to sign deals with each other to develop technology to ease the management of revoked certificates.

The goal is to develop software that will give corporations immediate access to the lists of certificates--used in public-key exchanges--that have been revoked and, in turn, guarantee that the people with whom they are dealing are authenticated.

Other than expiration dates, there is no current physical means to strip a digital certificate from an invalidated user's computer.

Lexis-Nexis, in Dayton, Ohio, provides digital certificates to law firms throughout the country. These firms, said David Vandagriff, director of technology alliances at Lexis-Nexis, can't afford any lag between the time a certificate is revoked and the time notification is sent to business partners.

"Because confidentiality is so important, the process of making sure people are authorized is critical," Vandagriff said. "I don't want to have to individually tell everyone to get rid of someone's public key in their E-mail."

Current revocation capabilities in applications aren't much better than the little black books merchants once used to check bad credit cards.

For example, VeriSign, of Mountain View, Calif., uses a CRL (Certificate Revocation List), a list of all VeriSign certificates that have been revoked for one reason or another, such as an employee leaving a company. It is displayed on a public Web site and routinely updated to servers at VeriSign customer sites.

As long as the certificate holders on both sides of a transaction are VeriSign customers, the CRL revocation list works fine. But, while VeriSign may be the biggest CA (certificate authority), it isn't the only one.

Most certificate services and software vendors rely on CRLs that don't interoperate. As a result, if a company issues its own digital certificates, it must let others know when one has been revoked.

Does that mean that digital certificates are insecure? Not necessarily. Most digital certificates have an expiration date and can be tied to a responsible CA or a corporation that issues certificates.

Revocation, on the other hand, is a security hole that should concern users.

Many of the security features in the upcoming release of Windows NT 5.0, due later this year, will focus on digital certificates. Microsoft is also working on certificate revocation options.

For starters, the company will ship its new Certificate Server 2.0 certificate management software with Windows NT 5.0 and integrate it with Windows NT's Active Directory, said Karan Khanna, product manager at Microsoft, in Redmond, Wash.

With that integration, Windows NT 5.0 will gain a CRL list. Microsoft's Internet Explorer 4.0 supports the company's existing Authenticode certificate revocation capabilities, though in default mode this capability is turned off. Internet Explorer will support CRLs later this year.

Netscape's Communicator client currently has limited support for revocation checking, though officials in Mountain View, Calif., say the company will improve CRL support in Navigator and Communicator by year's end.

On the server side, Netscape's Certificate Server currently supports CRLs and integrates them with Lightweight Directory Access Protocol directories.

VeriSign and other vendors are also working on the proposed OCSP (Online Certificate Status Protocol), which will allow an automatic check on a certificate's status.

However, the specification, under development by the Internet Engineering Task Force, is still months from completion. There also is concern that OCSP could be a bandwidth hog, since it establishes a second connection back to the server to check on a certificate's status.

For its part, ValiCert, of Sunnyvale, Calif., has created a certificate revocation tree, which would allow CRLs to interoperate, and has licensed its tool kit to GTE, Netscape, Entrust and others. Next quarter, GTE will release a tool kit that will allow its corporate customers to check the CRL listings.

IT departments, users say, should be cautious as they extend certificate services across the Internet. "A security breach," said Vandagriff, "always comes at the borders of technology."

COPYRIGHT 1998 Ziff-Davis Publishing Company

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: Ziff-Davis Publishing Company

EVENT NAMES: *220 (Strategy & planning)

GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372613 (Network Security Software); 9912610
(Information Systems)
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office
Automation)
NAICS CODES: 51121 (Software Publishers)

7/9/59 (Item 24 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

05380917 Supplier Number: 48182121 (THIS IS THE FULLTEXT)

Field Trials Set for Valicert's Certificate Validation System

KUTLER, JEFFREY

American Banker, p19

Dec 16, 1997

ISSN: 0002-7561

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 755

TEXT:

Less than two months since it officially opened for business, Valicert Inc. has announced global field trials for its digital certificate validation service.

Proponents of the technology say it could give Internet commerce a necessary boost, and Valicert's initial implementations could be an important proving ground.

The system revolves around technology called a certificate revocation tree, designed to overcome a flaw in the authentication process that many banks and other companies will be deploying as on-line commerce takes off.

Digital certificates, which can authenticate a computer user, are known to be valid at the time of issuance. Uncertainty creeps in at the time of a later transaction, however, and Valicert offers a way to test the validity.

Valicert said Monday it will operate the system on a service bureau basis, a program it markets under the name Valicert Service. This was not available in October when the Sunnyvale, Calif., company announced two other products, Valicert Toolkit and Valicert Server.

Three international certificate authorities will participate in the field trial beginning next month: Baltimore Technologies of Ireland, Belsign of Belgium, and Thawte of South Africa and the United States.

Baltimore Technologies operates the Eurotrust electronic commerce infrastructure serving the European Union and sees the "cooperation among leading security providers accelerating the global expansion of electronic commerce," said chief executive officer Fran Rooney.

"Valicert will provide an ideal opportunity to further explore the logistics and operational issues of a global certificate authority network," said Jack Nagle, general manager of Eurotrust Services.

These companies, well regarded in the data security industry, add to the credibility Valicert earned with a previously announced group of supporters: Entegrity Solutions, Entrust Technologies, GTE Corp.'s Cybertrust certificate authority unit, and Netscape Communications Corp.

Tom Carty, vice president of GTE, said his company intends to do pilots with Valicert. "It's great to see a compromise-recovery system in the marketplace," he said, adding it is probably better suited to electronic mail or financial service network security than for SET, the MasterCard-Visa certification standard that is already bolstered by an underlying transaction authorization infrastructure.

Belsign CEO Anthony Belpaire said the work with Valicert can help "make the Internet a safe place for electronic commerce."

"Given our focus on the creation of a simple, robust trust model for Internet commerce, the partnership with Valicert makes enormous sense as we cooperatively play a role in the growth of secure on-line commerce," said Thawte CEO Mark Shuttleworth.

Valicert president Joseph "Yosi" Amram and chairman Chini Krishnan use a credit card analogy to explain how certificate validation works.

"To be truly useful, a credit card must be able to be validated anywhere in the world, no matter where it was issued," Mr. Amram said. "In the same way, issuers and users of digital certificates need a quick and cost-effective clearing mechanism to assure the validity of these electronic credentials anywhere in the world."

The current reliance on unwieldy certificate revocation lists, or CRLs, is akin to retailers in the early days of credit cards checking each cardholder account number against those listed in a printed "hot card" bulletin.

The Valicert executives say their certificate validation method, based on an invention by the scientist who developed the security system used in Netscape browsers, is equivalent to on-line credit card authorizations. The Valicert Service is to certificate validation what a third-party processor such as First Data Corp. is to credit card authorization.

"The nice thing about the revocation tree is it minimizes bandwidth, has scalability, requires minimal processing, and is transparent to the user," Mr. Krishnan said.

Mr. Amram said he was not ready to announce pricing of Valicert Service, but "there will be different levels and some aspect of it is likely to be free."

The company adhered to a relatively nominal Internet pricing model for the tool kit, which is free for noncommercial downloading. Application development licenses are \$995 with unlimited sublicensing rights.

The Valicert Server cost for corporate intranets was \$9,995, and the package could be available from partner companies like Netscape or GTE on a reseller basis.

While Valicert enters into partnerships with such "industry insiders," Mr. Amram said likely initial buyers are banks and telecommunications companies that are developing certificate authorities, and potentially Internet service providers.

For the Valicert Service trial, live data will be fed in from existing certificate revocation lists. The company said the trial will be able to handle more than 30 million validation requests a day.

Copyright © 1997 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1997 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *Valicert Inc.

EVENT NAMES: *336 (Product introduction)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372691 (Data Encryption Software); 7372640

(Electronic Commerce Software)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: COMPANY

7/9/60 (Item 25 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

05305110 Supplier Number: 48076737 (THIS IS THE FULLTEXT)

Managing Digital Certificates; ValiCert unveils product, service suite

Yasin, Rutrell

InternetWeek, p52

Oct 27, 1997

ISSN: 1096-9969

Language: English Record Type: Fulltext

Document Type: Newsletter; Trade

Word Count: 379

TEXT:

By the year 2000, there will be millions of digital certificates in use. With that prediction in mind, users and vendors have begun to wonder how they are going to manage them all.

Getting a jump on the pack of vendors that hope to capture the certificate-management market, start-up ValiCert Inc. last week rolled out a suite of products and services designed to solve the certificate-revocation problem.

The ValiCert Toolkit, ValiCert Server and ValiCert Services will give users a way to distinguish between valid and compromised X.509 digital certificates in real time, according to Joseph "Yossi" Amram, ValiCert president and CEO.

Certificates-encrypted electronic signatures that bind a person's or a company's identity to a message or transaction--are an important component for security in transacting business over the Internet or corporate intranets.

Currently, security systems validate certificates by checking them against electronic lists of "bad numbers," known as certificate-revocation lists (CRLs). To verify a certificate, an administrator must obtain the latest list and then use memory-sapping software to sift through the list and ensure that the certificate in question is not on the list.

As the public key infrastructure grows, the number of certificates will expand beyond current systems, according to Michael Goulde, a senior analyst with the Patricia Seybold Group.

"As revocation lists get bigger and bigger, the present system is not going to work," Goulde said.

Anticipating a need for a more efficient way to validate certificates, ValiCert launched a "revocation tree" that delegates the job of list checking, Goulde said. This approach makes it easier to identify bad number information contained in multiple CRLs, he said.

Software developers can use the ValiCert Toolkit to embed certificate-validation capabilities into their user applications, ValiCert said.

ValiCert also launched the ValiCert Server, which builds a certificate revocation tree from a certificate revocation list.

ValiCert Services will act as a clearinghouse for checking the validity of certificates. Any application that uses ValiCert technology will be able to request verification of digital certificates from ValiCert servers, according to ValiCert officials.

The tool kit and server are available now; ValiCert Services will ship in the first quarter of 1998. The tool kit costs \$995. The server costs \$9,995 and supports Windows NT and Sun Solaris systems.

Copyright 1997 CMP Media Inc.

COPYRIGHT 1997 CMP Publications, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: CMP Media, Inc.

COMPANY NAMES: *Valicert Inc.

EVENT NAMES: *336 (Product introduction)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372691 (Data Encryption Software)

INDUSTRY NAMES: BUSN (Any type of business); TELC (Telecommunications)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: COMPANY

7/9/61 (Item 26 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

05300991 Supplier Number: 48070567 (THIS IS THE FULLTEXT)

Valicert Tackles Flaw in E-Commerce Security

KUTLER, JEFFREY

American Banker, p14

Oct 23, 1997

ISSN: 0002-7561

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 970

TEXT:

A group of Silicon Valley entrepreneurs has set out to correct a flaw in the digital certification process that many Internet experts have been counting on to make Internet commerce secure.

The solution, called a certificate revocation tree, is the property of Valicert Inc., a Sunnyvale, Calif., company formed last year and officially opened for business this week.

In a sign that Valicert may be on to something that could bring added security to Internet transactions, three vendors in the data encryption field have given endorsements, and Netscape Communications Corp. has made a provision for Valicert's technology to "plug in" to the SuiteSpot server software.

The advent of Valicert indicates that digital certification-a cryptographic technique that is believed to be on the road to broad public acceptance through Internet security protocols such as the credit card industry's SET-needs further refinement.

"Today there is no way to know if a certificate is valid at the time of a transaction-it is known only that the certificate was valid at the time of issuance," said Joseph "Yosi" Amram, president and chief executive officer of Valicert.

He said that if not for the Valicert method of keeping revoked certificates from being approved-it will be available in the form of a tool kit for system developers, a server system, and a service from Valicert-electronic commerce could collapse under the weight of millions of digital certificates that cannot be adequately validated.

SET, the Secure Electronic Transactions protocol adopted by MasterCard and Visa for on-line credit card transactions, illustrates the problem in the extreme. SET requires issuance of digital certificates to all parties to a transaction. They are the E-commerce equivalent of a driver's license to verify a cardholder's identity or a certification that an on-line merchant is what it claims to be.

The complexity of processing transactions with those multiple certificates is widely seen as slowing the adoption of SET.

But digital certificates have already been issued by the millions through Netscape and Microsoft Corp.'s Internet browsers. Verisign Inc. and GTE Corp. are prominent certificate vendors. GTE, Entegriety Solutions, and Entrust Technologies, the leader in public key infrastructure systems, have each agreed to some form of collaboration with Valicert.

Valicert's efforts can "expand the security infrastructure available for commerce," said Tom Carty, vice president of marketing and business development at GTE. "Given our focus on providing all of the pieces of the infrastructure required to make Internet commerce possible, it makes great sense for us to partner with Valicert to fill in one of the most essential pieces of the infrastructure puzzle-the digital credential checkpoint."

In a recent interview, Mr. Amram and Valicert chairman Chini Krishnan said the problem is akin to what the credit card industry faced before electronic authorization systems.

"A merchant would get a book, which came once a week or once a month, full of bad credit card numbers, and credit cards presented at the point of sale would have to be looked up manually," said Mr. Amram, who joined Valicert in August after being involved in other high-tech start-ups and in the Silicon Valley venture capital scene. "It was a big hassle and it slowed down checkout."

The digital certificate equivalent of the hot-card list is known as the certificate revocation list, or CRL.

Mr. Krishnan, the Valicert founder, said CRLs are "unscalable," meaning they become cumbersome, if not impossible, to manage as they approach mass-market proportions. The lack of scalability "has posed a barrier to widespread deployment," Mr. Krishnan said.

He claimed that the invention of the certificate revocation tree brings a "1,000-to-1 advantage" that solves the problem of revocation and validation in a tamper-proof and economical way.

"Developers need a cost-effective, one-step solution for building

applications that can check the validity of digital certificates," Mr. Amram said. "By providing a clearing house network into multiple certification authorities, and by delivering a robust technology combined with a liberal licensing policy, Valicert will enable the widespread development and use of applications that will make the Internet and corporate intranets safe to conduct business."

"Certificates are the only way to deal with identity in any meaningful way," Mr. Amram said. "They will take off in a big way. But certificates without validation are like a car without brakes."

Mr. Krishnan said the development of Valicert's technology had "a lot of rocket science elements," which is why it took the company 20 months to reach the launch stage. Enhancing its credentials, Paul Kocher, a leading cryptography researcher, is credited with inventing the underlying technology. Martin Hellman, a Stanford University professor and half of the Diffie-Hellman team that invented public key cryptography, is on Valicert's scientific advisory board.

Commercializers of cryptographic security have been intrigued by Valicert's proposition. When he heard about it during American Banker's Online '97 conference in Phoenix, Scott Dueweke, a marketing manager in International Business Machines Corp.'s Internet division, said, "They should call us."

Another expert, who asked not to be identified, said Valicert's biggest problem is that it is a few years ahead of its time.

"The market has fallen down with respect to revocation management, relying on relatively short expiration dates" to minimize invalid certificates, said Victor Wheatman, a California-based analyst with Gartner Group, Stamford, Conn. "Valicert fills a void and hopes to develop technology before the leading players move forward with their own revocation capabilities."

Valicert's server and tool kit are available now, and its service to certificate acceptors will enter field trials later this year, the company said. The tool kit can be downloaded from the valicert.com Web site free for noncommercial use and evaluation purposes. Application development licenses are a flat \$995 with unlimited sublicense rights. The server can be deployed on corporate intranets for \$9,995.

Copyright c 1997 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1997 American Banker-Bond Buyer

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: American Banker-Bond Buyer

COMPANY NAMES: *Valicert Inc.

EVENT NAMES: *336 (Product introduction)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372691 (Data Encryption Software)

INDUSTRY NAMES: BANK (Banking, Finance and Accounting); BUSN (Any type of business)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: COMPANY

7/9/92 (Item 27 from file: 16)

DIALOG(R) File 16:Gale Group PROMT(R)

(c) 2002 The Gale Group. All rts. reserv.

05294603 Supplier Number: 48061927 (THIS IS THE FULLTEXT)

Encryption Start-Up Serves Servers

Dunlap, Charlotte

Computer Reseller News, p24

Oct 20, 1997

ISSN: 0893-8377

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 270

TEXT:

Sunnyvale, Calif.: A new encryption start-up, launching today, aims to

provide a service that verifies the validity of digital certificates in realtime and offer toolkits and servers to VARs.

Staffed with a "Who's Who" of cryptography, ValiCert Inc., based here, will sell its toolkits to developers of commerce systems for added security. It also has signed deals with vendors, including Netscape Communications Corp., to embed ValiCert's encryption server technology into the vendors' servers. And finally, the company will provide a service to anyone involved in communicating via digital certificates, to immediately determine the validity of X.509 digital certificates.

"The core of our technology is the mathematical and cryptographic data infrastructure, called a certificate revocation tree," said Chini Krishnan, chairman, chief technology officer and founder of the company.

The technology securely transfers updated information regarding digital certificates to every computer on its server. ValiCert's technology is able to differentiate between valid and compromised digital certificates, he said.

Digital certificates are encrypted electronic "signatures" that attach the identification of a person or company to their electronic message or transaction.

Also on the ValiCert team are Paul Kocher, co-founder and chief scientist, who designed the cryptography for Netcape's current security technology, Secure Sockets Layer; and Marty Hellman, the co-inventor of public key cryptography, known as Diffie-Hellman.

The ValiCert Toolkit will be offered to VARs and software developers for an annual licensing fee of \$995.

Vendors, including Netscape will release a plug-in for the technology in future versions of its SuiteSpot servers. ValiCert initially will conduct field trials of its verification service, with broad availability slated for 1998.

Copyright 1997 CMP Media Inc.

COPYRIGHT 1997 CMP Publications, Inc.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: CMP Publications, Inc.

COMPANY NAMES: *ValiCert Inc.

EVENT NAMES: *360 (Services information)

GEOGRAPHIC NAMES: *1USA (United States)

PRODUCT NAMES: *7372691 (Data Encryption Software)

INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation)

NAICS CODES: 51121 (Software Publishers)

SPECIAL FEATURES: COMPANY

7/9/63 (Item 1 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter

(c) 2002 The Dialog Corp. All rts. reserv.

07610665 (THIS IS THE FULLTEXT)

E-commerce credit checks move into online markets.

Internet trade can be profitable only if online businesses are

John Gerald's.

NETWORK NEWS, p20

September 29, 1999

JOURNAL CODE: WNNS LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 237

US companies are setting themselves up as intermediaries that authenticate internet transactions between vendors and users.

The latest start-up in this market is ValiCert, which claims it can validate almost any digital certificate.

A recent report from analyst Aberdeen Group says that companies like ValiCert could prove a critical cog in the industry's electronic infrastructure.

Eric Hemmendinger, a senior analyst at Aberdeen Group and author of the report, told Network News last week: "As a neutral player among

multiple certificate authorities, companies like ValiCert are in a position today to provide enterprises with the products and services they need to enable a clearing house function for PKI based e-business."

Sathvik Krishnamurthy, Vali-Cert's vice president of marketing, said: "We are providing a similar service to the one used by the credit card industry, to combat fraud. The same level of security has to be applied to digital certificates."

Valicert's certificate authority software, ValiCert Enterprise VA 2.0, provides validity status responses for any X.509 certificate using a raft of current validation mechanisms.

These include Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), CRL Distribution Points (CRLDP) and Certificate Revocation Tree (CRT) validation.

The software includes components that work with e-mail clients, address books and browsers.

ValiCert currently licenses its technology to customers such as IBM, Oracle and the US Department of Defence. It is also helping Intel to develop its Common Data Security Architecture set of security protocols.

Copyright 1999 VNU Business Publications Ltd. Source : World Reporter (Trade Mark)

DESCRIPTORS: Company News; New Products & Services; Marketing

COUNTRY NAMES/CODES: United States of America (US)

REGIONS: Americas; North America; Pacific Rim

SIC CODES/DESCRIPTIONS: 7375 (Information Retrieval Services); 7372 (Prepackaged Software)

NAICS CODES/DESCRIPTIONS: 514191 (On-Line Information Services); 51121 (Software Publishers)

7/9/64 (Item 2 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter

(c) 2002 The Dialog Corp. All rts. reserv.

07297208

US start-up hopes to become fraud detector for online transactions

SECTION TITLE: News

John Gerald's in Silicon Valley

NEWSWIRE (VNU)

September 18, 1999

JOURNAL CODE: WNEW LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 356

A Silicon Valley start-up is attempting to set itself up as a third party intermediary between users and vendors to authenticate Internet transactions and communications between them. Three-year old ValiCert aims to address the problem of validating certificates for public key infrastructure (PKI) and digital certificate systems from almost any vendor by checking users identity and financial situation. Sathvik Krishnamurthy, ValiCert's vice president of marketing, said: "Our success depends on the ubiquity of our technology. We're providing a similar service to the one for the credit card industry, where you can get rid of fraud. That same thing has to happen in digital certificates." Earlier this year, the company introduced its certificate authority software, ValiCertEnterprise VA 2.0, which provides validity status responses for any X.509 certificate using a raft of current validation mechanisms. These include Certificate Revocation Lists (CRLs); Online Certificate Status Protocol (OCSP); CRL Distribution Points (CRLDP) and Certificate Revocation Tree (CRT) validation. The software includes an Email Validator, which plugs in to Secure Mime based email clients, an Address Book Validator, which regularly scans certificates within an email name and address book to see whether they are valid, and a Browser Validator, which alerts corporate users if commerce servers are using a Secure Sockets Layer certificate that has been revoked. And according to a report from The Aberdeen Group, ValiCert could provide a

critical component of an enterprise's Internet, intranet and extranet infrastructure. Eric Hemmendinger, a senior analyst at the Aberdeen Group and author of the report, said: "As a neutral player among multiple certificate authorities, ValiCert is in a position today to provide enterprises with the products and services they need to enable clearing house function for PKI based ebusiness." Certco and Computer Associates? Platinum unit are also developing ways to validate digital certificates, but ValiCert currently licenses its technology to customers such as IBM, Oracle, WorldTalk and the US Department of Defense. It is also helping Intel develop its Common Data Security Architecture set of security protocols. ValiCert has just raised \$23 million from strategic investors, bringing its venture funding up to \$30 million, which it will use to fund marketing programmes and international expansion.

Copyright 1999 VNU Business Publications Ltd. Source : World Reporter (Trademark)

COMPANY NAMES: Intel Corp
DESCRIPTORS: Company News; Contracts & New Orders; Patents Licensing & Standards
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
SIC CODES/DESCRIPTIONS: 7372 (Prepackaged Software); 7375 (Information Retrieval Services); 9631 (Regulation Administration of Utilities)

7/9/95 (Item 3 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter
(c) 2002 The Dialog Corp. All rts. reserv.

07241352 (THIS IS THE FULLTEXT)

Data Security Firm Adds Validation Function

SECTION TITLE: On-Line Banking

JEFFREY KUTLER

AMERICAN BANKER , v164, p14

September 16, 1999

JOURNAL CODE: WAMB LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 1105

Certco Inc. has added a powerful validation component to its digital trust technology.

The New York data security company, a spinoff of the former Bankers Trust Corp., introduced CertValidator, a system that assures the validity of a digital certificate presented in an electronic commerce transaction.

Certificate validation has become a critical issue -- for some, a stumbling-block -- in attempts to complete the construction of Internet commerce infrastructures.

In the digital equivalent of the printed credit card "hot lists" of the 1960s and 1970s, an on-line seller might have to consult an unwieldy certificate revocation list, or CRL, to see if a presented credential expired or was revoked. CRLs are widely considered unworkable for large-volume networks that put a premium on speed. A leading alternative is OCSP -- the on-line certificate status protocol -- on which CertValidator is built.

Vendors of public key encryption and digital certificate technologies have taken steps to accommodate non-CRL options like OCSP. Xcert International Inc. of Walnut Creek, Calif., has explicitly avoided CRLs because it views on-line, real-time status checking as essential. One company specializing in validation methods and related support services, Valicert Inc. of Mountain View, Calif., has raised consciousness about the issue with its own technology, certificate revocation trees, as well as OCSP.

Certco differs from Valicert's Validation Authority offering, said Certco senior vice president Jay Simmons, in that it integrates a secure OCSP data repository with the "responder" function.

Yosi Amram, president of Valicert, said, "I and Valicert welcome the

entry of Certco into the validation space.

"This helps to further legitimize the business need" and reinforces "a message that Valicert has been conveying to the market for over two years."

Calling CertValidator "the second leg of a product offering" that began with certificate authority systems, Mr. Simmons said, "We believe it will be necessary to know who issued a certificate and to get a positive response that it has been issued."

Among the key benefits would be nonrepudiation. A buyer of goods, for example, would be unable to claim improperly or fraudulently after the fact that the transaction did not occur.

In keeping with open interoperability principles, CertValidator can store and manage certificates, CRLs, and status data from all major certificate authority vendors. The president of one of them, Peter Hussey of GTE Corp.'s Cybertrust unit, said the program fits well with its "secure extranet" offerings. "This powerful technology not only gives our customers a flexible option for accelerating their business-to-business e-commerce activities," Mr. Hussey said, "but it also makes them more secure."

"Real-time validation capability within and across public key infrastructures is critical for businesses that intend to engage in high-value e-business transactions via the Internet," said Diana Kelley, senior security analyst with Hurwitz Group Inc. "OCSP support and multivendor interoperability are features that the market should demand."

Richard Salz, the architect of CertValidator, said the system's foundations in standards such as OCSP and LDAP (lightweight directory access protocol) and certification for meeting high-level Federal Information Processing Standards contribute to the all-important flexibility and scalability requirements sought by customers.

Included on a long list of CertValidator operational features are hardware-based data encryption and key storage, tamper-proofing, audit trails, and two trademarked ideas, Fast-Path Revocation and Fast-Path Suspension. The former occurs much faster than the hours or days that a CRL system might take. With the latter, a hold can be placed on a certificate in a critical situation, then quickly lifted to return it to valid status.

Meridien Research senior analyst Octavio Marenzi said OCSP responders and repositories can meet the instantaneous information needs of trading partners only if they are "highly secure, fully interoperable, and scalable. All (those) characteristics appear to be present" in CertValidator.

Certco president and chief executive officer John Herron said CertValidator is an "industrial-strength implementation of OCSP," resulting from the company's mix of skills in such areas as cryptography, banking, law, software, and risk management.

"Many of our technical advantages are simple in design yet sophisticated in concept, the product of engineers and others who know a lot more than just technology," Mr. Herron said.

Mr. Simmons said the system is not only designed "as a secure repository for managing certificate life cycles across multiple certificate authorities," but also is well suited for "the Identrus model" -- a certificate infrastructure that requires multiple participating banks to be in sync with validation.

Certco, in fact, was instrumental in the formation last year of Identrus LLC, a multinational business-to-business trust consortium that included among the founders Bankers Trust and its Germany-based acquirer, Deutsche Bank.

Mr. Simmons said he views Identrus as one of the likely sparks to growth in commercial use of public key encryption technologies in the coming year. "Y2K will be behind us, and we see the banks moving very aggressively," he said.

Certco relinquished its shareholder position in Identrus to compete on an even footing for the banks' business. A rival, Baltimore Technologies, was designated root-key supplier for the pilot phase, and Valicert won a role for its validation tools.

Mr. Amram described CertValidator as "effectively an OCSP responder product," whereas his company, Valicert, is already into a "third generation" with a multipronged strategy including a server that supports

all protocols and a third-party validation authority service.

"OCSP is a key component of Identrus' risk management strategy," said the consortium's chief operations and technology officer, Kristin Kupres. "It's great to see Certco respond to the need for real-time digital certificate validation by advancing this important standard."

?

MOUNTAIN VIEW, Calif. -- The Validation technology supplier Valicert Inc. said it has obtained \$23 million in a mezzanine round of venture capital financing.

Leading the investment group was Lucent Venture Partners, an arm of Lucent Technologies. Other members included Canadian Imperial Bank of Commerce, Financial Technology Ventures, First Analysis, France Telecom, Gemplus, Korea Technology Banking, Mitsui, and Thomson-CSF Ventures.

This money came on top of \$7 million last year from August Capital, Bessemer Venture Partners, Draper Fisher Jurvetson, Intel, and U.S. Venture Partners, all of which were also in the mezzanine round.

"This round of funding will enable Valicert to greatly extend the availability of its Validation Authority solutions, allowing companies around the world to securely conduct business transactions over the Internet," said Jean-Michel Barbier, president of Thomson-CSF Ventures, the investment unit of the French technology company.

Valicert president and chief executive officer Yosi Amram said he is "excited at the breadth and diversity of our new investor syndicate. We expect their financial, technology, and distribution experience to play a critical role as we continue to add value to our business."

Copyright c 1999 American Banker, Inc. All Rights Reserved.
http://www.americanbanker.com

Copyright 1999 American Banker, Inc. a division of Thomson Inform.

Source: World Reporter (Trade Mark).

COMPANY NAMES: Bankers Trust Corp

DESCRIPTORS: Company News; New Products & Services; Marketing

COUNTRY NAMES/CODES: United States of America (US)

REGIONS: Americas; North America; Pacific Rim

SIC CODES/DESCRIPTIONS: 6211 (Security Brokers & Dealers); 7372

(Prepackaged Software)

7/9/66 (Item 4 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter

(c) 2002 The Dialog Corp. All rts. reserv.

05284763 (THIS IS THE FULLTEXT)

Valicert in Pacts with 4 Foreign Certificate Firms

SECTION TITLE: Technology

JEFFREY KUTLER

AMERICAN BANKER , v164, p17

March 02, 1999

JOURNAL CODE: WAMB LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 622

Valicert Inc. of Mountain View, Calif., announced cooperation agreements Monday with four international information security companies, a sign of the rapid spread of digital certificate technology in foreign markets.

Valicert, which supports the part of the certificate process known as validation, has forged alliances with such U.S.-based vendors as Entegritty Solutions Corp., Entrust Technologies Inc., GTE Internetworking, Intel Corp., and Netscape Communications Corp.

But Valicert and its marketing partners are encountering considerable demand for certificate services elsewhere, particularly in Europe, said Yosi Amram, president and chief executive officer.

Underlining that trend, Valicert is establishing or expanding relationships with four companies that are selling digital certificate products and are based in other countries: Baltimore Technologies of

Ireland and the United Kingdom, GlobalSign of Belgium, Thawte Certification of South Africa, and Software Agencies Australia, which is known as SAA.

Mr. Amram said the deals are the fruit of a marketing effort led by Alexander Garcia-Tobar, vice president of international. The two previously worked together at another Silicon Valley venture, Individual Inc. Mr. Garcia-Tobar more recently was the architect of Forrester Research Inc.'s international expansion.

His arrival at Valicert last summer was timely, Mr. Amram said, because Europe's digital certificate and public key infrastructure market "is neck and neck with, if not ahead of, the United States in terms of adoption and development."

"Culturally, the Europeans are more security- and privacy-conscious," he said. "They are further along with smart cards, which creates a good foundation for a certificate-based infrastructure and applications."

And in the Asia-Pacific region, countries such as Australia, Malaysia, and Singapore have launched large-scale public key infrastructure (PKI) and electronic commerce initiatives.

Valicert expects its validation business to grow hand-in-hand with digital certificates, which are data encryption-related credentials for authenticating parties in an electronic transaction. Valicert sells the concept of a validation authority, or VA. It would complement the certificate authority, or CA, which is gaining credence through the efforts of companies like Baltimore, Entrust, and Verisign Inc.

Valicert promotes a technique for ascertaining a certificate's validity- assuring that it is not expired or revoked-called a certificate revocation tree. But the company's products also support OCSP-on-line certificate status protocol-and the certificate revocation list, or CRL, approach.

"Valicert is the recognized leader in digital certificate validation, and we felt confident in completely outsourcing our global validation requirements to them," said Thawte president and CEO Mark Shuttleworth.

With the Valicert Global VA service, he said, customers will be assured of "complete validation integrity" while Thawte can "differentiate its service and focus on its core business of certification."

Mr. Amram said Thawte, No. 2 to Verisign in issuing certificates under the Internet's popular SSL security protocol, is well advanced in cross-certification among different CAs. That could be a boon to Valicert as well.

GlobalSign, formerly Belsign, is No. 3 in public SSL certificates. It will be a Valicert distributor, use Global VA with a CRL system, and bring Valicert into its GlobalSign Ready interoperability program. GlobalSign CEO Anthony Belpaire said the choice of Valicert "is the first step in ensuring that our customers will have instant access to the best validation products on the market.

SAA will be a Valicert distributor for Australia and New Zealand, which Mr. Garcia-Tobar described as "important emerging markets for PKI."

Valicert contributes to SAA's strategy of providing "leading-edge electronic commerce solutions with a universal, scalable family of products," said SAA managing director Bob White.

Baltimore "is licensing and embedding our tool kit and using our VA server as their validation solution," Mr. Amram said. One of the fastest-growing certificate companies, Baltimore was named with GlobalSign as CA subcontractors for a major European Union commerce project coordinated by PricewaterhouseCoopers. Copyright c 1999 American Banker, Inc. All Rights Reserved. <http://www.americanbanker.com>

Copyright 1999 American Banker, Inc. a division of Thomson Inform.
Source: World Reporter (Trade Mark).

DESCRIPTORS: Joint Ventures; Strategy; Company News

COUNTRY NAMES/CODES: United States of America (US) ; Ireland (IE) ;
United Kingdom (GB) ; Belgium (BE) ; South Africa (ZA)

REGIONS: Americas; North America; Pacific Rim; Europe; European Union;
Western Europe; Africa; Sub-Saharan Africa

SIC CODES/DESCRIPTIONS: 3674 (Semiconductors & Related Devices)

7/9/67 (Item 5 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter
(c) 2002 The Dialog Corp. All rts. reserv.

03826833 (THIS IS THE FULLTEXT)

Validation Vendor in Deal with GTE Unit

SECTION TITLE: Technology

JEFFREY KUTLER

AMERICAN BANKER , v163, p10

December 22, 1998

JOURNAL CODE: WAMB LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 502

Valicert Inc. has gained an attractive outlet for its digital validation technology by signing a formal alliance agreement with the GTE Cybertrust unit of GTE Internetworking.

As a major source of public key infrastructure systems for Internet commerce security, GTE Cybertrust gives Valicert a valuable credibility boost.

Valicert-which has been working at least informally with GTE, Entrust Technologies Inc., Baltimore Technologies, and others in the data security field-is purveyor of a technique called CRT for ascertaining whether a digital certificate is valid.

CRT, for certificate revocation tree, is touted as more streamlined than the certificate revocation lists, or CRLs, incorporated in conventional models of the digital authentication technology. CRLs are seen as too unwieldy and unreliable for the stressful, high-volume conditions that are expected to develop with mass-market on-line commerce.

For the certificate authority that manages the intricacies of issuing and verifying digital credentials, GTE Cybertrust can add Valicert to its service menu and has rights to resell the two-year-old validation company's Enterprise Server. The system can check revocation status by any standard means including CRL, CRT, and On-line Certificate Status Protocol.

"Digital certificate validation is critical to enterprises implementing open PKI (public key infrastructure) solutions to secure transactions among large numbers of users, including employees, customers, partners, and suppliers," said Joe Vignaly, director of marketing and business development for GTE Cybertrust, Needham Heights, Mass.

As a Valicert reseller, "Cybertrust meets the growing needs of our customers," he said, "...by providing a one-stop source for both CA (certificate authority) products and services and certificate validation."

"GTE participated in our field trial before this, but now we have a more formal relationship," said Sathvik Krishnamurthy, vice president of marketing and business development for Valicert in Mountain View, Calif. "GTE is the largest company we have done a distribution agreement with." Another is Entegriety Solutions Corp. of San Jose, Calif.

"Our goal is to make our validation solution ubiquitous, and that requires relationships with CAs and tool kit licensees" such as GTE and Intel Corp., Mr. Krishnamurthy added.

Like others in information security, Mr. Krishnamurthy can sound like an evangelist on the subject of "an expanded definition of trust" for electronic commerce. "Our agreements with CAs like GTE reinforce that notion," he said in an interview.

The CRL processing challenge has daunted system developers. Valicert offers one solution. In November, Entrust Technologies of Texas announced several licensing agreements for its CRL Distribution Points patent, a "scalability" measure that Valicert president Yosi Amram said he could support.

Others have proposed different approaches that would do away with revocation lists altogether. But Mr. Krishnamurthy pointed out that virtually all major CA proposals, including the Global Trust Enterprise that eight multinational banks announced in October, are following de facto standards that have validation components.

"A variety of techniques are on offer," said analyst David Ferris of Ferris Associates, San Francisco. Focusing on "an important part of the PKI puzzle, Valicert is carving itself a useful little niche." Copyright c 1998 American Banker, Inc. All Rights Reserved. <http://www.americanbanker.com>

Copyright 1998 American Banker, Inc. a division of Thomson Inform.
Source: World Reporter (Trade Mark).

COMPANY NAMES: GTE Internetworking; GTE Corp
DESCRIPTORS: Marketing; Company News; Sales; Product Management
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
SIC CODES/DESCRIPTIONS: 7372 (Prepackaged Software)

7/9/98 (Item 6 from file: 20)
DIALOG(R) File 20:Dialog Global Reporter
(c) 2002 The Dialog Corp. All rts. reserv.

01939442 (THIS IS THE FULLTEXT)

Rajiv Dholakia Joins ValiCert as Vice President of Product Development and Operations

PR NEWSWIRE

June 16, 1998 8:18

JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 808

PALO ALTO, Calif., June 16 /PRNewswire/ -- ValiCert, Inc., the leading supplier of software and services for validating digital certificates, today announced that Rajiv Dholakia has joined as vice president of product development and operations. In his new capacity, Dholakia will be responsible for leading ValiCert's development of high-performance products and services for managing and validating digital certificates used in electronic commerce and communications.

"Rajiv is a very welcome addition to ValiCert's management team and provides strong leadership to our world-class engineering team," said Yosi Amram, president and CEO of the company. "His experience in developing Internet-based communications products will be invaluable to ValiCert as the company continues to deliver new generations of software and services that enable secure commerce and communications over the Internet."

"I am very pleased to have joined ValiCert," said Dholakia. "The company is a pioneer in the emerging area of digital certificate validation and provides a compelling opportunity to develop products and services that advance the use of the Internet as a secure platform for delivering services to business and

Prior to ValiCert, Dholakia was vice president of product development for TestDrive Software where he led the delivery of a cryptographically secure digital container-based e-commerce system focused on the online sale and super-distribution of digital content such as software. He also pioneered the development of a key digital rights management system based on x.509 certificate technology.

Previously, Dholakia led several projects at VillageTree Software, a consulting firm to start-up Internet companies. He has also served as director of engineering for platform products at Taligent, Inc., where he was responsible for delivering the Taligent CommonPoint products for Windows NT, OS/2, MacOS and Solaris.

He holds a B.E. degree in chemical engineering from Maharaja Sayajirao University of Baroda, India and did graduate work in applied artificial intelligence at the University of South

Digital Certificate Validation

Digital certificates are being used increasingly as electronic credentials for identification, for payment, and for other communications or business transactions conducted over the Internet or corporate intranets. As with the credit card industry, which developed a way to electronically validate the millions of credit card numbers issued by any

bank in the world, the use of digital certificates requires its own clearinghouse network for certificate confirmation so that individuals and businesses can assure the validity of any certificate.

ValiCert's Award-Winning Solution

ValiCert's software and services deliver the only universal, high-performance solution available today for validating digital certificates. ValiCert's products and services enable organizations to securely and rapidly manage the validation of digital certificates, and provide enterprise developers and ISVs with the tools to build applications that incorporate certificates. ValiCert's products and services include:

- * The ValiCert Universal Toolkit(TM) that provides developers with comprehensive off-the-shelf software components for easily building Internet/intranet applications that validate digital certificates using an array of established validation mechanisms;

- * The ValiCert Enterprise Server(TM) that works with any certificate issuance system to enable high-performance, interoperable certificate validity confirmation; and

- * The ValiCert Global Service(TM) that enables enterprises conducting broad-based Internet communications and commerce to check the validity of digital certificates across organizational boundaries. A global field trial of the ValiCert Service involving more than a dozen Certificate Authorities (CAs) and leading electronic vendors is currently under way.

The company's products this year received the 1998 Network Magazine Product of the Year Award in the Digital Certification category, and were named as the top choice in the security products category in Data Communications magazine's sixth annual Hot Products issue.

About ValiCert

ValiCert is the leading provider of solutions for validating digital certificates. ValiCert's software and services deliver a universal, high-performance solution for assuring the integrity of secure communications and electronic commerce transactions over the Internet. The company's products support all current approaches for digital certificate validation, including Certificate Revocation Lists (CRLs), the emerging OCSP standard, plus its own unique Certificate Revocation Tree(TM) (CRT) mechanism. ValiCert has partnerships with leading worldwide providers of security services and products. The company is headquartered in Palo Alto, Calif. and is available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

ValiCert, ValiCert Universal Toolkit, ValiCert Enterprise Server, ValiCert Global Service and Certificate Revocation Tree are trademarks of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

/CONTACT: Patrick Corman, for ValiCert, Inc., 650-326-9648,
patrick@cormancom.com/ 08:00 EDT

Copyright 1998 PR Newswire. Source: World Reporter (Trade Mark).

DESCRIPTORS: On the Move

7/9/99 (Item 7 from file: 20)

DIALOG(R)File 20:Dialog Global Reporter
(c) 2002 The Dialog Corp. All rts. reserv.

01487728 (THIS IS THE FULLTEXT)

Electronic Commerce: To Drum Up Interest, Valicert Is Giving Away Its Tool Kit

SECTION TITLE: Digital Frontiers

JEFFREY KUTLER

AMERICAN BANKER , v163, p13

April 28, 1998

JOURNAL CODE: WAMB LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 560

Hoping to put some added momentum behind its digital certification

tool, Valicert Inc. is offering its customers more options at a lower price.

Free, to be exact.

The Palo Alto, Calif., company announced the release last week of version 2.0 of its tool kit, which software developers can use to test for certificate revocation within electronic commerce programs.

Valicert contends that digital certificates, the electronic credentials that can verify buyers' and sellers' identities on the Internet, will reach their potential only if accompanied by a highly effective means of ascertaining that a given certificate has not expired or otherwise been revoked.

By giving away its software-it can be downloaded from the valicert.com Web site-Valicert is following a high-tech precept for stimulating market development. That could lead to sales of higher-end products for implementing certificate validation. "Getting the tool kit out develops ubiquity and a PKI," or public key infrastructure, Yosi Amram, the company's president and chief executive officer, said in an interview.

In theory, as on-line commerce and associated certificate volumes expand, system operators would then want to buy the high performance levels of Valicert's server system. Or a company validating certificates across business units might turn to Valicert's service bureau.

While the free distribution may be the main attention-grabber, Valicert may be making an even more significant gesture by rendering its tool kit "universal." It will support any validation protocol and not just the "certificate revocation tree" that Valicert champions.

The 2.0 tool kit thus will accommodate certificate revocation lists, or CRLs, which Valicert has dismissed as a slow legacy technology that will not stand up to the stresses of high-volume commerce. Valicert will also support OCSB, the On-line Certificate Status Protocol, being developed under the auspices of the Internet Engineering Task Force.

Any application developer, whether working on secure virtual private networks or the MasterCard-Visa SET payment protocol, "can use our tool kit to check the validity of any certificate, regardless of the platform they support," Mr. Amram said.

The openness "reflects our ongoing commitment to meeting developers' needs today and in the future for multiple validation and revocation technologies," the Valicert CEO added.

Mr. Amram said legacy systems will have a "clear migration path" to certificate revocation trees or beyond. He views the more elaborate OCSB as "right for high-value financial transactions" such as wholesale wire transfers, where people will be willing to pay a price, including a delay in response time, for a desired level of assurance.

"We have a system of roads that support Ferraris, Chevys, and buggies," he said. "For validation we need the equivalent. For some very high percentage of transactions-I don't know if it is 92%, 95%, 98%-certificate revocation tree is right."

Mr. Amram said market feedback since Valicert started selling its systems last year was favorable, but there was reluctance to "get on the bandwagon of a proprietary solution. "Now anyone has an easy, free, no-risk tool that is open and universal, supporting any protocol."

"Any tool kit has to embrace whatever method is being embraced by the marketplace for revocation management," said Victor Wheatman, an analyst with the Gartner Group of Stamford, Conn. "Valicert is continuing and extending its strategy of addressing revocation management, and the addition of protocols is appropriate."

The move won praise from the Financial Services Technology Consortium, the cooperative research organization of major U.S. banking companies. FSTC president Adam Backenroth of Chase Manhattan Corp. said it "demonstrates the true interoperability that is crucial for the global adoption of electronic commerce in the banking and financial services industry." Copyright c 1998 American Banker, Inc. All Rights Reserved. <http://www.americanbanker.com>

Copyright 1998 American Banker, Inc. a division of Thomson Inform.
Source: World Reporter (Trade Mark).

COMPANY NAMES: Valicert Inc; Chase Manhattan Corporation; Gartner Group Inc; MASTERCARD INTERNATIONAL LTD.; VISA INTERNATIONAL
DESCRIPTORS: Corporate Sales; Customer Base
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America
SIC CODES/DESCRIPTIONS: 7372 (Prepackaged Software)

7/9/70 (Item 1 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

11452702 SUPPLIER NUMBER: 56981210 (THIS IS THE FULL TEXT)
Valicert System No Longer a Niche Product; As Electronic Commerce Expands, So Does Need to Augment Digital Certificates.
Kutler, Jeffrey
American Banker, 164, 208, 22
Oct 28, 1999
ISSN: 0002-7561 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1143 LINE COUNT: 00099

TEXT:

Valicert Inc. and its validation technology for digital certificates are no longer being relegated to technically obscure roles in electronic commerce security.

The Mountain View, Calif., company has just begun shipping the latest version of its validation authority, or VA, system. With the announcement came several indications that the company's notion of validation, something of a tough sell when it was new and not widely understood, is finding a place in the quickly evolving Internet security infrastructure.

What Valicert calls its third-generation Enterprise VA Suite 3.0 gets much deeper into business practices than just ascertaining that a digital credential has not expired or been revoked -- the basic definition of certificate validation.

The package has several "application level" features that go to the heart of what banks and other companies want to be doing on the World Wide Web. And in a tangible sign of business progress by Valicert, its technology is being incorporated in significant e-commerce efforts such as the Identrus multinational banking consortium, the U.S. government's ACES -- Access Certificates for Electronic Services -- project, and various aspects of the Sun-Netscape Alliance, which is an e-commerce venture of Sun Microsystems Inc. and America Online Inc.'s Netscape Communications subsidiary.

Officials of Valicert, which in September raised \$23 million in mezzanine-stage financing from an international group led by Lucent Venture Partners, say three years of hard work in system development and market education are paying off.

Also in September, the company announced the opening of a European headquarters in Amsterdam, which president and chief executive officer Yosi Amram termed "another step in our mission to build a global validation network for secure e-commerce."

The digital certificates that many banks, government entities, and other "trusted third parties" view as a key to authenticating on-line trading partners will have to go through a validation step, the reasoning goes.

"The coming explosion in business-to-business transactions" will need this "critical enabler," said Valicert vice president of marketing and business development Sathvik Krishnamurthy. "Only Valicert is offering a complete, proven solution."

Among those sending kudos Valicert's way was Scott Lowry, president and CEO of Digital Signature Trust Co., a subsidiary of Zions Bancorp. of Salt Lake City and one of the first two vendors selected to provide the data encryption backbone for the government's ACES program.

Valicert's Enterprise VA Suite will be a part of the public key

infrastructure systems of both Digital Signature Trust and the other approved ACES vendor, Operational Research Consultants Inc.

"With its third-generation product," Mr. Lowry said, "Valicert has shown the ability to provide the robust validation capabilities that may be required by a project of such magnitude as ACES." The program sets a standard for management of digital certificates to ensure secure communications between citizens and the government.

Daniel E. Turissini, vice president of Operational Research Consultants, said, "Because of the multivendor nature of this project, it is crucial to have universal validation services, and Valicert is the perfect solution."

The validation vendor is not alone in offering this service. Certco Inc. of New York recently added a validation component based on the OCSP -- On-line Certificate Status Protocol -- to its digital trust technology offering.

But Valicert has attempted to set a standard for flexibility and compatibility. It worked to make its VA interoperable with all major providers of certificate authority, or CA, systems, among them Baltimore Technologies, Entrust, GTE Cybertrust, Thawte, and Verisign.

"We are viewed as a trusted third party, neutral, because we are not competing as a CA," said Ram Krishnan, Valicert's director of product marketing.

David Ferris, president of Ferris Research, a San Francisco-based firm focusing on messaging technologies, said, "This is an important niche, dominated by one vendor, Valicert. It's strange the firm doesn't have any real competition."

Valicert's VA "provides a clearing-house function for users of digital-certificate-based applications," said Eric Hemmendinger, senior analyst at Aberdeen Group of Boston. "Automatically confirming the validity of digital certificates issued by multiple suppliers' CAs, the VA provides a valuable form of insurance critical for enterprises conducting e-business."

Mr. Krishnan said the company is also "agnostic" when it comes to technical protocols for validation. It will support CRL, or Certificate Revocation Lists; the CRL-Distribution Points variation; OCSP; and Certificate Revocation Trees, a Valicert invention.

"The mission always has been to validate any certificate, from any CA, any protocol, anywhere on the planet," Mr. Krishnan said. "It is tough to make that claim. We are backing it up."

Valicert is billing Enterprise VA Suite 3.0 as "the first complete, universal certificate validation solution."

Among the enhancements to one of the components, the server system that has been on the market two years, is a mechanism called Stateful Validation. Going beyond simple certificate verification, it enables validation of "things specific to the application's context," Mr. Krishnan said. In other words, the system can verify an aspect of a transaction other than a credential's validity, inquiring into a credit bureau or human resources data base, for example.

Valicert has described its validation function as equivalent to a credit card authorization. Mr. Krishnan extended the analogy for Stateful Validation: "It tells you not only that the credit card is good, but that the customer is authorized to buy \$5,000 of stuff."

Enterprise VA 3.0 has been enhanced to serve networks of certificate authorities operating in multiple locations, such as Identrus. Banks will be both competing with each other and cooperating to obtain validations, which the Valicert framework can accommodate.

There is also a feature called Enterprise VA Mirroring, which enables data to be replicated or shared efficiently among several validation authorities that may be scattered around the world.

Such capabilities add up to "more integration (of VA) with business applications," Mr. Krishnan said. "The power of what we do is only as good as the applications we are supporting," and they range from Web servers and browser software to virtual private networks and secure e-mail.

"Customers really seem to be excited," Mr. Krishnan added. He said Valicert's selection for the forthcoming Identrus pilot and its signing of

one of that consortium's founding banks, ABN Amro, will be followed by more banking industry contract announcements.

"We are feeling good that our message is getting out to the financial services industry," Mr. Krishnan said. "It is critically important to secure what they do, and they realize that their certificate technology is incomplete without validation."

Copyright c 1999 American Banker, Inc. All Rights Reserved.

<http://www.americanbanker.com>

COPYRIGHT 1999 American Banker-Bond Buyer

COMPANY NAMES: Valicert Inc.--Products

INDUSTRY CODES/NAMES: BANK Banking, Finance and Accounting; BUSN Any type of business

DESCRIPTORS: Computer software industry--Products; Electronic commerce--Computer programs

GEOGRAPHIC CODES/NAMES: 1USA United States

PRODUCT/INDUSTRY NAMES: 7372000 (Computer Software)

EVENT CODES/NAMES: 330 Product information

NAICS CODES: 51121 Software Publishers

FILE SEGMENT: TI File 148

7/9/71 (Item 2 from file: 148)

DIALOG(R) File 148:Gale Group Trade & Industry DB

(c)2002 The Gale Group. All rts. reserv.

09960615 SUPPLIER NUMBER: 20130972 (THIS IS THE FULL TEXT)

ValiCert Announces Robert L. Ross as Vice President of Business Development

PR Newswire, pl08SEFMTH01

Jan 8, 1998

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 371 LINE COUNT: 00037

TEXT:

PALO ALTO, Calif., Jan. 8 /PRNewswire/ -- ValiCert, a company delivering encryption technology and services for assuring the validity of digital certificates, today announced that Robert L. Ross has joined the company as vice president of business development. Bringing more than ten years of experience in business development and marketing, Ross will be responsible for developing strategic relationships and managing all business development activity.

Prior to joining ValiCert, Ross headed media business development at Marimba, Inc. where he directed all business initiatives for the media marketplace. Before Marimba, he spent more than six years at Individual, Inc., most recently as director of strategic business development where he developed product and marketing partnerships with leading Internet service and content providers, including Microsoft Corporation, Yahoo! and Netscape Communications Corporation. He also marketed and sold Individual's business intelligence solutions into Fortune 1000 enterprise accounts. Prior to Individual, Ross held technical marketing positions roles at Apple Computer. "Robert Ross brings to ValiCert a unique blend of business, technology, and marketing experience," said Yosi Amram, president and CEO of ValiCert. "With his experience at Marimba, Individual and Apple, Robert demonstrated his ability to think strategically and to forge key deals and partnerships -- skills that will now help us build ValiCert into an even more important force in the marketplace."

Ross earned a B.A. degree in political science from Duke University.

About ValiCert

ValiCert was established in 1996 by a group of leading cryptographers and executives from the Internet services industry to build a broad validation infrastructure for the net economy. Utilizing technology based on an innovative cryptographic technique called certificate revocation trees, ValiCert delivers an efficient, scalable and transparent solution for checking the validity of digital certificates in any Internet or intranet transaction. ValiCert is headquartered in Palo Alto, Calif. and is

available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

SOURCE ValiCert, Inc.

-0-

01/08/98

/CONTACT: Patrick Corman of Corman Communications, 650-326-9648, or corman@cerfnet.com, for ValiCert/

/Web site: <http://www.valicert.com/>

CO: ValiCert, Inc. ST: California IN: CPR SU: PER

TW-KW -- SFMTH01 -- 5899 01/08/98 18:43 EST <http://www.prnewswire.com>

COPYRIGHT 1998 PR Newswire Association, Inc.

COMPANY NAMES: Valicert Inc.--Officials and employees

INDUSTRY CODES/NAMES: BUS Business, General; BUSN Any type of business

DESCRIPTORS: Computer software industry--Officials and employees

PRODUCT/INDUSTRY NAMES: 7372691 (Data Encryption Software)

SIC CODES: 7372 Prepackaged software

FILE SEGMENT: NW File 649

7/9/72 (Item 3 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2002 The Gale Group. All rts. reserv.

09933310 SUPPLIER NUMBER: 20087751 (THIS IS THE FULL TEXT)

ValiCert Launches Global Field Trial of First Digital Certificate Validation Service

PR Newswire, p1215LMM005

Dec 15, 1997

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 1225 LINE COUNT: 00115

TEXT:

Collaboration with International CAs Baltimore, BelSign and Thawte to Kick-Off

Global Validation Service for Digital Certificates

SUNNYVALE, Calif., Dec. 15 /PRNewswire/ -- ValiCert, a company delivering encryption technology and services for assuring the validity of digital certificates, today announced global field trials of the first certificate validation service, the ValiCert Service(TM), in partnership with leading digital certificate providers from Europe and South Africa. Initial participants in the field trial include international certificate authorities (CAs) Baltimore Technologies (Ireland and the European Union), BelSign (Europe) and Thawte (South Africa/USA).

ValiCert's global field trial will provide validation of digital certificates using live data, aggregating an array of certificate revocation list (CRL) data from ValiCert's CA service partners. These CA service partners will use the ValiCert Service to provide scalable validation services to assure the validity of their customers' certificates across the global Internet. The CA service partners will feed all live data from their CRLs into the ValiCert Service.

The ValiCert Service trial provides a unique opportunity for application developers, enterprises deploying a public key infrastructure, as well as users of certificate-enabled applications and services to test them in a real-world setting using the first available global validation service. The trial will be capable of managing an average transaction rate of more than 30 million certificate validation requests per day.

"To be truly useful, a credit card must be able to be validated anywhere in the world, no matter where it was issued," said Yosi Amram, president and CEO of ValiCert, Inc. "In the same way, issuers and users of digital certificates need a quick and cost-effective clearing mechanism to assure the validity of these electronic credentials anywhere in the world. The ValiCert service easily scales to meet the requirements of today's global economy, and provides the first effective worldwide system to validate digital certificates."

ValiCert's field trial will begin in January 1998. For information about the ValiCert field trial, see <http://www.valicert.com>.

Collaboration With Industry Leaders

"We are extremely pleased to partner with this group of leaders in the digital certification industry for our initial field trials," said Chini Krishnan, chairman and chief technology officer of ValiCert. "This collaborative effort is an essential part of ValiCert's goal of supporting a robust, scalable validation infrastructure."

ValiCert's CA partners in these trials -- Baltimore Technologies, BelSign and Thawte -- are among the earliest issuers of digital certificates to businesses and individuals.

Baltimore Technologies is a global developer of information security products and services for electronic commerce and Internet business. From their headquarters in Dublin, Baltimore Technologies operates the EuroTrust Trusted Third Party (TTP) infrastructure for electronic commerce throughout the EU. "Baltimore Technologies is excited by ValiCert's global field trial and feel that this co-operation between leading security providers will accelerate the global expansion of electronic commerce," said Fran Rooney, CEO of Baltimore Technologies."

"EuroTrust is at the leading edge of developing a pan-European Trusted Third Party infrastructure exploring aspects of cross certification and authentication," said Jack Nagle, general manager EuroTrust Services. "ValiCert will provide an ideal opportunity to further explore the logistics and operational issues of a global CA network."

BelSign issues digital certificates for individuals and corporations to secure business and personal transactions across the Internet and intranets. "BelSign is providing an easy and convenient way to ensure that the participants in an electronic transaction can trust each other," said Anthony Belpaire, CEO of BelSign. "We look forward to working with ValiCert in offering an important value-added service that will make the Internet a safe place for electronic commerce."

Thawte is a global provider of security and privacy products and services. "Thawte offers a complete suite of certification services to individuals and organizations," said Mark Shuttleworth, president and CEO of Thawte. "Given our focus on the creation of a simple, robust trust model for Internet commerce, the partnership with ValiCert makes enormous sense as we cooperatively play a role in the growth of secure online commerce."

The ValiCert Service

The ValiCert Service is a scalable and network-efficient system for enterprises that are conducting communications and commerce across the Internet. The service enables certificate issuers to distribute all revocation data confirming the validity of a digital certificate in a timely, secure manner. It makes this data -- traditionally associated with unscalable, network-intensive certificate revocation lists -- easily available to applications and people that they wish to conduct business with around the world. It enables any application, server or person accepting certificates, regardless of its source, to be assured of the certificate's validity.

The ValiCert Service is targeted at enterprises that are conducting broad-based Internet communications and commerce, as well as individuals using public certificate authorities. Commercial availability of the service is slated for 1998.

The ValiCert Service is part of the company's comprehensive suite of offerings for certificate validity management, that also includes the ValiCert Toolkit(TM) and the ValiCert Server(TM).

The ValiCert Toolkit is targeted at software developers writing applications that consume certificates. By embedding the toolkit into their applications, vendors enable products to efficiently check certificate validity in Internet or intranet communications.

The ValiCert Server is targeted at enterprises that deploy certificate systems and provides all the technology necessary for confirmation issuance in an intranet setting. The ValiCert Server can also be embedded in certificate issuance and management systems utilized by third-party certificate authorities.

Digital Certificates

Digital certificates are gaining momentum and acceptance for use as electronic credentials for identification (comparable to a driver's license or employee ID badge), for payment (comparable to a credit card), and for other communications or business transactions conducted over the Internet or corporate intranets today. As with the credit card industry, which developed a way to electronically validate the millions of credit card numbers issued by any bank in the world, the use of digital certificates requires its own clearinghouse network for certificate confirmation, so that individuals and businesses can assure the validity of any certificate.

About ValiCert

ValiCert was established in February 1996 by a group of leading cryptographers and executives from the Internet security industry to build a broad validation infrastructure for electronic commerce. Utilizing technology based on an innovative cryptographic technique called certificate revocation trees, ValiCert delivers an efficient, scalable and transparent solution for checking the validity of digital certificates in any Internet or intranet transaction. The company is collaborating with a number of industry partners including Entegriety Solutions, Entrust Technologies, GTE CyberTrust and Netscape(R) Communications Corporation.

ValiCert is headquartered in Sunnyvale, Calif. and is available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

ValiCert, ValiCert Server, ValiCert Toolkit and the ValiCert Service are trademarks of ValiCert, Inc. Netscape is a trademark of Netscape Communications Corporation, which is registered in the United States and other jurisdictions.

SOURCE ValiCert

-0-

12/15/97

/CONTACT: Patrick Corman of Patrick Corman Marketing & Communications, 650-326-9648, or corman@cerfnet.com/

CO: ValiCert ST: California IN: CPR MLM SU: PDT

GJ-DB -- LAMM005 -- 7362 12/15/97 09:17 EST <http://www.prnewswire.com>

COPYRIGHT 1997 PR Newswire Association, Inc.

COMPANY NAMES: Valicert Inc.--Product development

INDUSTRY CODES/NAMES: BUS Business, General, ~~BUSN~~ Any type of business

DESCRIPTORS: Cryptography equipment industry--Product development

PRODUCT/INDUSTRY NAMES: 3662627 (Encryption/Decryption Equip)

SIC CODES: 3663 Radio & TV communications equipment

FILE SEGMENT: NW File 649

7/9/73 (Item 4 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2002 The Gale Group. All rts. reserv.

09799501 SUPPLIER NUMBER: 19901981 (THIS IS THE FULL TEXT)

ValiCert Opens for Business to Offer New Solutions for Validating Digital Certificates

PR Newswire, p1020LAMM005

Oct 20, 1997

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 1188 LINE COUNT: 00112

TEXT:

Company Receives Broad Support From Industry-Leading Companies for Solving

Key Barrier to Secure Internet Communications and Transactions

SUNNYVALE, Calif., Oct. 20 /PRNewswire/ -- ValiCert, Inc., a new company delivering encryption technology and services for assuring the validity of digital certificates, today began operations and introduced a comprehensive suite of offerings for certificate validity management, consisting of the ValiCert Toolkit(TM), the ValiCert Server(TM) and the ValiCert Service(TM). The company today also announced the support of

several key industry partners including Entegriety Solutions, Entrust Technologies, GTE CyberTrust and Netscape(R) Communications Corporation.

Founded by some of the world's leading cryptographers, ValiCert's goal is to develop a broad certificate validation and revocation infrastructure for the Internet. The company's technology and services enable users to determine, in a time-critical manner, the validity of X.509 digital certificates for secure electronic communications and commerce. ValiCert's technology achieves this by differentiating between valid and compromised digital certificates -- encrypted electronic "signatures" that bind a person's or server's identity to a message or transaction. Until the availability of ValiCert's products, there has been no efficient way to check the validity or revocation status of digital certificates which are being used increasingly to authenticate electronic communications and transactions over the Internet and intranets.

"Users of digital certificates today face a problem similar to the one users of credit cards faced 25 years ago before automated authorization," said Chini Krishnan, founder and chairman of ValiCert. "Merchants had to manually verify each credit card presented to them using a cumbersome, outdated printed list of bad numbers.

"Similarly, certificate acceptance has entailed the use of large, unscalable certificate revocation lists, or CRLs, which has posed a barrier to their widespread deployment. ValiCert's technology removes this barrier by making it quick and painless to verify, during a transaction, the status of any digital certificate."

Prof. Martin Hellman, co-inventor of public key cryptography, added, "solving the issue of certificate compromise is central to building a reliable authentication infrastructure for secure communications and commerce. ValiCert addresses a basic and troublesome roadblock associated with digital certificates in a truly novel way." Dr. Hellman is part of ValiCert's scientific advisory board, and has been instrumental in reviewing, refining and promoting ValiCert's technology.

"The industry anticipates that by the end of this century, hundreds of millions of digital certificates will be in use," said Yosi Amram, president and CEO of ValiCert. "Without the robust, scalable validation infrastructure that ValiCert is providing, it will be impossible to manage this tremendous volume effectively."

ValiCert Products

ValiCert is introducing three core products centered around certificate validity management: ValiCert Server, ValiCert Toolkit and the ValiCert Service.

The ValiCert Toolkit(TM) is targeted at software developers writing applications that consume certificates. By embedding the toolkit into their applications, vendors enable products to efficiently check certificate validity in Internet or intranet communications. ValiCert also provides a comprehensive developer's guide, fully documented code and access to on-site consulting services.

The ValiCert Server(TM) is targeted at enterprises that deploy certificate systems and provides all the technology necessary for confirmation issuance in an intranet setting. The ValiCert Server constructs a certificate revocation tree from a certificate revocation list, and when requested by client application programs, constructs and issues confirmation of digital certificate status. The ValiCert Server will also be embedded in certificate issuance and management systems utilized by public certificate authorities (CAs).

The ValiCert Service will be targeted at enterprises that are conducting broad-based Internet communications and commerce. It will be a clearinghouse for checking the validity of digital certificates across organizational boundaries. The service will enable certificate issuers to distribute their certificate revocation lists in a timely, secure manner and to make them easily available to applications and people they wish to conduct business with around the world. It will also enable any application accepting certificates, regardless of its source, to be assured of the certificate's validity.

ValiCert's Certificate Revocation Tree

ValiCert's technology solves what is known as the certificate

revocation problem. This problem arises because applications that accept certificates need to determine not only that the certificate presented was in good standing at the time of issuance, but also that the certificate has not been revoked subsequently and is valid at the time of acceptance.

The current solution for managing certificate revocation is to maintain electronic lists of bad numbers, called certificate revocation lists (CRLs), which can become very large, cumbersome and difficult to download and process in real time. An application needing to verify a digital certificate must obtain the latest list from the appropriate list issuer, and plow through the list to ensure that the certificate in question is not on the list. This process is slow, inefficient, unscalable and bandwidth intensive. It makes revocation checking unsuitable for mass-market electronic commerce transactions and secure communications.

ValiCert's technology solves the certificate revocation problem more efficiently by using a new cryptographic technique called a certificate revocation tree. This technique allows anyone with a digital certificate to pre-approve the certificate with a very small piece of tamper-proof data that proves the validity of the certificate beyond doubt to a recipient. Furthermore, because this data is very cheap to construct and process and the cost of the system only scales as the logarithm of the number of revoked certificates, certificate revocation trees are a basis for a truly scalable, global validation infrastructure on the Internet. More information on the mathematics and cryptographic basis of certificate revocation trees is available from ValiCert's site at <http://www.valicert.com>.

Product Availability

The ValiCert Server and ValiCert Toolkit are available now. Field trials of the ValiCert Service will begin later this year.

About ValiCert

ValiCert was established in February 1996, by a group of leading cryptographers and executives from the Internet security industry to build a broad validation infrastructure for electronic commerce. Utilizing technology based on an innovative cryptographic technique called certificate revocation trees, ValiCert delivers an efficient, scalable and transparent solution for checking the validity of digital certificates in any Internet or intranet transaction. ValiCert is headquartered in Sunnyvale, Calif. and is available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

ValiCert, ValiCert Toolkit, ValiCert Server and ValiCert Service are trademarks of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

SOURCE ValiCert, Inc.

-0-

10/20/97

/NOTE TO EDITORS: see October 20, 1997 press releases entitled, "ValiCert Announces the Availability of Digital Certificate Validation Toolkit and Server(TM)" and "ValiCert Working With Entrust Technologies, GTE, and Integrity Solutions to Define and Build Certificate Validation Infrastructure."/

/CONTACT: Patrick Corman of Patrick Corman Marketing & Communications 650-326-9648 or corman@cerfnet.com/

CO: ValiCert, Inc. ST: California IN: CPR MLM TLS SU: JVN PDT

MZ-TR -- LAMM005 -- 7176 10/20/97 09:03 EDT <http://www.prnewswire.com>

COPYRIGHT 1997 PR Newswire Association, Inc.

COMPANY NAMES: Valicert Inc.--Management

INDUSTRY CODES/NAMES: BUS Business, General; BUSN Any type of business

DESCRIPTORS: Computer software industry--Management

PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software); 7372691 (Data Encryption Software)

SIC CODES: 7372 Prepackaged software

FILE SEGMENT: NW File 649

7/9/74 (Item 5 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09799500 SUPPLIER NUMBER: 19901980 (THIS IS THE FULL TEXT)
**ValiCert Announces Availability of Digital Certificate Validation Toolkit
and Server Toolkit Enables Certificate Validation Checking in
Applications;**

PR Newswire, p1020LAMM004

Oct 20, 1997

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 1144 LINE COUNT: 00106

TEXT:

Server Issues and Streamlines Validation Confirmations
SUNNYVALE, Calif., Oct. 20 /PRNewswire/ -- ValiCert, Inc., a new company delivering encryption technology and services for assuring the validity of digital certificates, today announced the availability of its ValiCert Toolkit(TM) and ValiCert Server(TM) products. The ValiCert Toolkit enables developers to integrate X.509-compliant digital certificate validity checking capabilities into applications that consume certificates, such as Web servers and browsers, virtual private networks, EDI and payment systems, and e-mail clients and servers. The ValiCert Server works with certificate servers and provides them with the capability to effectively issue certificate validation confirmations.

Digital certificates -- attachments to electronic messages used to verify that a user sending a message is who he or she claims to be -- are gaining increasing momentum and acceptance for use as general purpose credentials in Internet communication and transactions. But like other credentials, they can be lost, stolen or otherwise invalidated, and thus revoked by the issuing authority. Until now, there has been no efficient and scalable way to check, during a transaction, whether a digital certificate is valid. ValiCert's technology solves this problem by providing a quick and efficient way to check the status of a digital certificate, effectively shielding certificate holders and acceptors alike from the misuse of compromised credentials.

"Developers today need a cost-effective, one-stop solution for building applications that can check the validity of digital certificates," said Yosi Amram, president and CEO of ValiCert. "By providing a clearinghouse network into multiple certificate authorities, and by delivering a robust technology combined with a liberal licensing policy, ValiCert will enable the widespread development and use of applications that will make the Internet and corporate intranets a safe place to conduct business."

"Infrastructure solutions for electronic commerce must work with all computing devices and in all types of networking environments," said Paul Kocher, a leading cryptography researcher and the inventor of the technology underlying ValiCert's products. "ValiCert will succeed because it offers the first truly cross-platform, multi-environment solution for what could otherwise be an overwhelming problem."

ValiCert Toolkit

The ValiCert Toolkit enables developers to easily build applications based on ValiCert's certificate revocation tree technology, a cryptographic technique that is recognized by many security experts as the basis for a truly scalable, worldwide certificate validation system. Using the toolkit, developers can provide applications, such as Web browsers and servers, e-mail clients and others, with the seamless capability to check the validity of digital certificates in an online, time-critical manner. The ValiCert Toolkit also includes a comprehensive developer's guide, fully documented code and access to on-site consulting services.

The ValiCert Toolkit is designed to work with the ValiCert Service, or with any certificate server or certificate management system that incorporates the ValiCert Server.

ValiCert Server

The ValiCert Server is designed to work with certificate issuance systems and is a solution for providing validity confirmations in a secure,

efficient and scalable manner.

The ValiCert Server constructs certificate revocation trees from CRLs, and when requested by the Toolkit, creates and issues verifications for digital certificates within an intranet environment. The ValiCert Server also provides a link between the intranet and ValiCert's service by uploading and aggregating revocation data for distribution on the Internet. The ValiCert Server is licensed directly to corporate customers, and on an OEM basis to product vendors and certificate authorities (CAs).

ValiCert's Approach to Certificate Revocation

ValiCert's technology solves the certificate revocation problem, i.e., the ability to determine during a transaction not only that a digital certificate was issued in good standing some time in the past, but also that the certificate is valid and has not been revoked at the time of acceptance. The current solution for managing certificate revocation is to maintain electronic lists of bad numbers, called certificate revocation lists (CRLs), which are large and cumbersome, and difficult to download and process in real time. An application needing to verify a digital certificate must obtain the latest list from the appropriate list issuer, and plow through the list to ensure that the certificate in question is not on the list.

This process is slow, inefficient, unscalable and bandwidth-intensive, making revocation checking unsuitable for mass-market electronic commerce transactions and secure communications.

ValiCert's technology solves the certificate revocation problem more efficiently with a new cryptographic technique called a certificate revocation tree. This technique allows anyone with a digital certificate to pre-approve the certificate with a very small piece of tamper-proof data that proves the validity of the certificate. Furthermore, because this data is very cheap to construct and process, and the cost of the system only scales as the logarithm of the number of revoked certificates, certificate revocation trees are the basis for the first truly scalable, global validation infrastructure on the Internet.

More information on the mathematics and cryptographic characteristics of certificate revocation trees is available from ValiCert's site at <http://www.valicert.com>.

Availability

~~The ValiCert Toolkit is available now and is free for non-commercial~~ use and evaluation. The product can be downloaded from ValiCert's web site located at <http://www.valicert.com>. Application development licenses for the ValiCert Toolkit are \$995 per year for an unlimited number of end-user application licenses.

The ValiCert Server is licensed on an OEM basis to certificate authorities or sold directly to companies operating their own CAs in an Intranet setting. Contact ValiCert at info@valicert.com for pricing details.

About ValiCert

ValiCert was established in February 1996, by a group of leading cryptographers and executives from the Internet security industry to build a broad validation infrastructure for electronic commerce. Utilizing technology based on an innovative cryptographic technique called certificate revocation trees, ValiCert delivers an efficient, scalable and transparent solution for checking the validity of digital certificates in any Internet or intranet transaction. ValiCert is headquartered in Sunnyvale, Calif. and is available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

ValiCert, ValiCert Toolkit, ValiCert Server and ValiCert Service are trademarks of ValiCert, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

SOURCE ValiCert, Inc.

-0-

10/20/97

/NOTE TO EDITORS: See October 20, 1997 press releases entitled, "ValiCert Opens for Business to Offer New Solutions for Validating Digital Certificates," and "ValiCert Working With Entrust Technologies, GTE and Entegrity Solutions to Define and Build Certificate Validation Infrastructure."/

/CONTACT: Patrick Corman of Patrick Corman Marketing & Communications, 650-326-9648, corman@cerfnet.com/
CO: ValiCert, Inc. ST: California IN: CPR SU: PER
TR-MZ -- LAMM004 -- 7171 10/20/97 09:03 EDT http://www.prnewswire.com
COPYRIGHT 1997 PR Newswire Association, Inc.

COMPANY NAMES: Valicert Inc.--Product introduction
INDUSTRY CODES/NAMES: BUS Business, General; BUSN Any type of business
DESCRIPTORS: Computer software industry--Product introduction
PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software); 7372510 (Software Development Tools)
SIC CODES: 7372 Prepackaged software
FILE SEGMENT: NW File 649

7/9/75 (Item 6 from file: 148)

DIALOG(R) File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09799499 SUPPLIER NUMBER: 19901979 (THIS IS THE FULL TEXT)
ValiCert Working With Entrust Technologies, GTE and Entegritty Solutions to Define and Build Certificate Validation Infrastructure
PR Newswire, p1020LAMM003
Oct 20, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1112 LINE COUNT: 00105

TEXT:

Industry Collaboration Expected to Accelerate Adoption and Use of Digital

Certificates

SUNNYVALE, Calif., Oct. 20 /PRNewswire/ -- ValiCert, Inc., a new company delivering cryptographic technology and services for assuring the validity of digital certificates, today announced a collaboration with several of the industry's leading infrastructure and digital certificate providers including Entrust Technologies, GTE and Entegritty Solutions. ValiCert will work with these companies to conduct global field trials of its certificate validation services, and to integrate and co-market its offerings with these companies' products. Netscape(R) Communications Corporation also announced the availability this month of ValiCert plug-ins that work with Netscape(R) SuiteSpot server software to enable efficient certificate revocation checking.

ValiCert's products and services are focused on assuring the validity of certificates in transactions and messaging on the Internet and intranets. The company's products introduced today include the ValiCert Server(TM), ValiCert Toolkit(TM) and the ValiCert Service(TM).

"We view our technology and services for certificate validity management as unique and essential to the authentication process of commerce and secure communications," said Chini Krishnan, chairman and chief technology officer of ValiCert. "We are truly pleased to be working with this distinguished set of vendors to solve this critical problem."

"Netscape was among the first to recognize certificate technology as an effective, interoperable security solution that is both easy to deploy and easy to use across platforms," said Taher Elgamal, chief scientist at Netscape. "The ValiCert plug-ins make it easy for Netscape customers to deploy ValiCert certificate validation technology with Netscape software on intranets, extranets, and the Internet." The plug-ins are expected be available from ValiCert at no charge later this month through <http://www.valicert.com> or through <http://developer.netscape.com>.

Entrust Technologies, GTE and Entegritty Solutions, all leaders in products and services for encrypted communications and electronic commerce infrastructure, are working with ValiCert to enhance the scalability and manageability of digital certificates in Internet communications and transactions.

Entrust Technologies, a leading provider of public cryptography products for encryption, digital signatures, and automated key management for both Internet and intranet applications, supports ValiCert's efforts to provide a value-added certificate validation service. "Entrust products orchestrate end-to-end security for enterprises across multiple applications spanning both the Internet and intranets," said Brian O'Higgins, chief technology officer, Entrust Technologies. "Certificate validation is an important value-added service for electronic commerce."

Added John Weinschenk, vice president of marketing at Entegriety Solutions, a recognized security development platform in the security tools marketplace, "Entegriety Solutions is committed to offering its customers best of breed, modular and interoperable solutions for all aspects of the digital certificate infrastructure. We view our relationship with ValiCert as essential to that commitment and look forward to contributing our expertise to this dynamic team to solve the global certificate revocation problem. In the immediate near future, we plan to integrate ValiCert's new cutting-edge technology into Entegriety's Security Development Platform (SDP)."

"GTE is committed to providing its customers with the best and broadest certificate infrastructure solutions in the industry," said Tom Carty, vice president of marketing and business development at GTE. "As a leader in providing certification authority products and services, GTE is encouraged by, and supports the valuable work being done by ValiCert to expand the security infrastructure available for commerce. Given our focus on providing all of the pieces of the infrastructure required to make Internet electronic commerce possible, it makes great sense for us to partner with ValiCert to fill in one of the most essential pieces of the infrastructure 'puzzle' -- the digital credential check point. We look forward to working with ValiCert to refine the infrastructure for secure online commerce."

ValiCert's technology and services are based on a new cryptographic technique, known as certificate revocation trees, that allow for a highly scalable, efficient and secure solution to certificate validation. "By providing efficient and time critical validity services for live certificates, ValiCert will accelerate the adoption of Internet public key infrastructure," said Yosi Amram, president and CEO of ValiCert. "We are targeting our offerings at vendors that provide products and services for operating certificate authorities (CAs), such as Entrust Technologies, GTE, and Entegriety solutions; to the leading platform companies, such as Netscape; as well as to companies that develop communications and commerce applications."

Digital Certificates

Digital certificates are gaining momentum and acceptance for use as electronic credentials for identification (comparable to a driver's license or employee ID badge), for payment (comparable to a credit card), and for other communications or business transactions conducted over the Internet or corporate intranets today. As with the credit card industry, which developed a way to electronically validate the millions of credit card numbers issued by any bank in the world, the use of digital certificates requires its own clearinghouse network for certificate confirmation, so that individuals and businesses can assure the validity of any certificate.

About ValiCert

ValiCert was established in February 1996, by a group of leading cryptographers and executives from the Internet security industry to build a broad validation infrastructure for electronic commerce. Utilizing technology based on an innovative cryptographic technique called certificate revocation trees, ValiCert delivers an efficient, scalable and transparent solution for checking the validity of digital certificates in any Internet or intranet transaction. ValiCert is headquartered in Sunnyvale, Calif. and is available on the World Wide Web at <http://www.valicert.com>, or by e-mail at info@valicert.com.

ValiCert, ValiCert Server, ValiCert Toolkit and the ValiCert Service are trademarks of ValiCert, Inc. Netscape is a trademark of Netscape Communications Corporation, which is registered in the United States and other jurisdictions.

Netscape, Netscape Navigator and the Netscape N logo are registered trademarks of Netscape Communications Corporation in the United States and other countries. Other Netscape logos and Netscape product and service names are also trademarks of Netscape Communications Corporation, which may be registered in other countries. All other product names are trademarks of their respective owners.

SOURCE ValiCert, Inc.

-0-

10/20/97

/NOTE TO EDITORS: See October 20, 1997 press releases entitled, "ValiCert Opens for Business to Offer New Solutions for Validating Digital Certificates," and "ValiCert Announces Availability of Digital Certificate Validation Toolkit and Server."/

/CONTACT: Patrick Corman of Patrick Corman Marketing & Communications 650-326-9648 or corman@cerfnet.com/

CO: ValiCert, Inc. ST: California IN: CPR MLM TLS SU: JVN PDT

MZ-TR -- LAMM003 -- 7174 10/20/97 09:03 EDT http://www.prnewswire.com

COPYRIGHT 1997 PR Newswire Association, Inc.

COMPANY NAMES: Valicert Inc.--Product development; Entrust Technologies Inc.--Product development; GTE Corp.--Services; Entegritiy Solutions Corp --Product development

INDUSTRY CODES/NAMES: BUS Business, General; BUSN Any type of business

DESCRIPTORS: Computer software industry--Product development; Telecommunications industry--Services

PRODUCT/INDUSTRY NAMES: 7372613 (Network Security Software); 4811500 (Specialized Telecommunication Services)

SIC CODES: 7372 Prepackaged software; 4822 Telegraph & other communications

TICKER SYMBOLS: GTE

FILE SEGMENT: NW File 649

7/9/76 (Item 1 from file: 256)

DIALOG(R) File 256:SoftBase:Reviews,Companies&Prods.

(c)2002 Info.Sources Inc. All rts. reserv.

00116344

DOCUMENT TYPE: Review

PRODUCT NAMES: ValiCert Enterprise VA 2.0 (747505)

TITLE: Enterprise suite lends validity to certificates

AUTHOR: Balfour, Gail

SOURCE: Computerworld Canada, v15 n3 p28(1) Feb 12, 1999

ISSN: 1484-9089

HOME PAGE: http://www.lti.on.ca

RECORD TYPE: Review

REVIEW TYPE: Product Analysis

GRADE: Product Analysis, No Rating

ValiCert's ValiCert Enterprise VA 2.0 works with a user's certificate authority software to provide validity status responses for any X.509 certificate. It uses many modern validation methods, including Certificate Revocation Lists (CRLs), On-line Certificate Status Protocol (OCSP), RL Distribution Points (RLDP), and ValiCert's Certificate Revocation Tree (CRT). Online and offline status checking are supported, and an E-Mail Validator is included that plugs into Secure/Multipurpose Internet Mail Extensions) (S/MIME) e-mail clients. Also provided are an Address Book Validator that scans certificates within an e-mail name and address took to determine if they are validated, and a Browser Validator that allows end-users to be notified if a commerce server is using a Secure Sockets Layer certificate that has been revoked. A new Validator Toolkit allows integration into applications, and a VA Publisher distributes regularly updated CRL information from multiple CAs to ValiCert's server. On-Line

Certificate Status Protocol support is also new to ValiCert Enterprise, as are plug-ins to certificate-supported applications, including Outlook 98, Windows Address Book, and multiple Web servers and browsers.

COMPANY NAME: ValiCert (639273)

SPECIAL FEATURE: Screen Layouts

DESCRIPTORS: Computer Security; Communications Protocols; Internet Utilities; E-Mail Utilities; Internet Security

REVISION DATE: 20010331

?